On divisors of terms of linear recurrence sequences

By *C. L. Stewart* *) at Waterloo

1. Introduction

Let r and s be integers with r^2+4s non-zero. Let u_0 and u_1 be integers and put

$$u_n = r u_{n-1} + s u_{n-2},$$

for $n=2, 3, \ldots$. Then for $n \geqq 0$ we have

$$u_n = a\alpha^n + b\beta^n, \tag{1}$$

where α and β are the two roots of x^2-rx-s and

$$a = \frac{u_0\beta - u_1}{\beta-\alpha}, \quad b = \frac{u_1 - u_0\alpha}{\beta-\alpha},$$

whenever $\alpha \neq \beta$. 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 $\frac{\alpha}{\beta}$ is not a root of unity.

In 1934 Mahler [7], [9] showed, by a p-adic generalisation of the Thue-Siegel theorem, that the greatest prime factor of u_n, the n-th term of a non-degenerate binary recurrence sequence, tends to infinity with n. However, because of the ineffective nature of the Thue-Siegel-Roth theorem, Mahler's proof does not yield an effective lower bound, which tends to infinity with n, for the greatest prime factor of u_n. In 1967 Schinzel [16], by employing a p-adic theorem of Gelfond in place of the p-adic Thue-Siegel Theorem used by Mahler, was able to give such a 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

$$P(u_n) > C n^{c_1} (\log n)^{c_2}, \tag{2}$$

where $C = C(r, s, u_0, u_1)$, c_1 and c_2 are effectively computable positive numbers; indeed we may take $c_1 = \frac{1}{84}$ and $c_2 = \frac{7}{12}$ if α and β are integers, $c_1 = \frac{1}{133}$ and $c_2 = \frac{7}{19}$ otherwise.

*) This research was supported in part by Grant A 3528 from the Natural Sciences and Engineering Research Council of Canada.

0075-4102/82/0333-0002$02.00

In this article we shall obtain estimates from below for the greatest prime factor of u_n and the greatest square-free factor of u_n, when u_n is the n-th term of a linear recurrence sequence. For any integer m let $Q(m)$ denote the greatest square-free factor of m with the convention that $Q(0)=Q(\pm 1)=1$. Thus if $m=p_1^{h_1}\cdots p_r^{h_r}$ with $p_1,\ldots,p_r$ distinct primes and $h_1,\ldots,h_r$ positive integers then $Q(m)=p_1\cdots p_r$. In our first theorem we improve on Schinzel's estimate (2).

Theorem 1. *Let u_n, defined as in* (1), *be the n-th term of a non-degenerate binary recurrence sequence and let d denote the degree of α over the rational numbers. Then*

$$P(u_n)>C_1\left(\frac{n}{\log n}\right)^{\frac{1}{d+1}},\quad Q(u_n)>C_2\left(\frac{n}{(\log n)^2}\right)^{\frac{1}{d}}, \tag{3}$$

where C_1 and C_2 are positive numbers which are effectively computable in terms of a and b only.

We remark that if α and β are real quadratic irrational numbers then Theorem 4 gives a better lower estimate for $Q(u_n)$ in terms of n than Theorem 1 does.

Let a, b, x and y be non-zero integers with $x\neq\pm y$. Since ax^n+by^n is the n-th term of the recurrence sequence defined by the relation $u_n=(x+y)\,u_{n-1}-xyu_{n-2}$ with initial terms $u_0=a+b$ and $u_1=ax+by$, we have, for any integer n larger than one,

$$P(ax^n+by^n)>C_3\left(\frac{n}{\log n}\right)^{\frac{1}{2}},$$

and

$$Q(ax^n+by^n)>C_4\frac{n}{(\log n)^2},$$

where C_3 and C_4 are positive numbers which are effectively computable in terms of a and b only. Our proof of Theorem 1 depends upon estimates for linear forms in the logarithms of algebraic numbers, due in the complex case to Baker [1] and in the p-adic case to van der Poorten [13].

A Lucas sequence is a non-degenerate binary recurrence sequence $(t_n)_{n=0}^{\infty}$ with $t_0=0$ and $t_1=1$. For such sequences the results of Theorem 1 can be improved. It follows from results of Schinzel, Shorey and Stewart [17], [18], [22] and [23] that if t_n is the n-th term of a Lucas sequence then

$$P(t_n)\geqq\max\left\{n-1,\ C_5\frac{n\log n}{(q(n))^{\frac{4}{3}}}\right\},$$

for $n>C_6$, where $q(n)$ denotes the number of square-free divisors of n, C_6 is an absolute constant and C_5 is a positive number which is effectively computable in terms of α and β only.

We are able to strengthen (3) by means of an elementary argument, whenever u_n is non-zero and is divisible by a prime number p which does not divide u_m, for any non-zero u_m with $0\leqq m<n$. We shall call such a prime number p a characteristic divisor of u_n. Our definition extends that of Carmichael [4] who defined characteristic divisors for Lucas sequences.

Theorem 2. *Let u_n be the n-th term of a non-degenerate binary recurrence sequence, defined as in* (1), *and put $v_n = b\alpha^n + a\beta^n$ for $n \geqq 0$. Let p be a characteristic divisor of u_n for $n > 3$. Then*

$$p \geqq n - C_7, \tag{4}$$

where C_7 is a positive number which is effectively computable in terms of a and b only. Further, if $u_m v_m \neq 0$ for all $m \geqq 0$ then

$$p \geqq n + [C_8 \log n],$$

where C_8 is a positive number which is effectively computable in terms of a, b, α and β.

Birkhoff and Vandiver [3] and Zsigmondy [26] proved that if a and b are coprime non-zero integers with $a \neq \pm b$ then $u_n = a^n - b^n$ has a characteristic divisor for $n > 6$. Similar results have been obtained for the Lucas numbers, see [17] and [23], although no comparable result is known in general. Ward [25] proved that for each non-degenerate binary recurrence sequence $(u_n)_{n=0}^{\infty}$ there are infinitely many prime numbers which divide at least one non-zero term of the sequence. Thus, from (4),

$$P(u_n) > n - C_7,$$

for infinitely many integers n. In fact, we are able to obtain the following stronger assertion, again by an elementary argument.

Theorem 3. *Let $(u_n)_{n=0}^{\infty}$ be a non-degenerate binary recurrence sequence. For all integers n, except perhaps for a set of asymptotic density zero,*

$$P(u_n) > \varepsilon(n)\, n \log n, \tag{5}$$

where $\varepsilon(n)$ is any real valued function for which $\lim_{n\to\infty} \varepsilon(n) = 0$.

For the case of a non-degenerate Lucas sequence Shorey and Stewart, [18] and [22], proved that (5) applies with $\varepsilon(n) n \log n$ replaced by $\dfrac{\varepsilon(n)\, n (\log n)^2}{\log\log n}$.

For general linear recurrence sequences much less is known. Let $r_1, \ldots, r_k$ and $u_0, \ldots, u_{k-1}$ be integers and put

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

for $n = k, k+1, \ldots$. We shall denote the field of rational numbers by $\mathbb{Q}$. It is well known, see page 62 of [6], that

$$u_n = f_1(n)\, \alpha_1^n + \cdots + f_t(n)\, \alpha_t^n, \tag{6}$$

where $f_1, \ldots, f_t$ are non-zero polynomials in n with degrees less than $l_1, \ldots, l_t$ respectively and with coefficients from $\mathbb{Q}(\alpha_1, \ldots, \alpha_t)$ where $\alpha_1, \ldots, \alpha_t$ are the non-zero roots of the characteristic polynomial

$$X^k - r_1 X^{k-1} - \cdots - r_k,$$

and $l_1, \ldots, l_t$ are their respective multiplicities. We shall say that the sequence $(u_n)_{n=0}^{\infty}$ is non-degenerate if $t>1$ and α_i, for $1 \leqq i \leqq t$, and α_i/α_j for $1 \leqq i < j \leqq t$ are different from roots of unity. In 1935 Mahler [8] proved that if $(u_n)_{n=0}^{\infty}$ is a non-degenerate linear recurrence sequence then $|u_n|$ tends to infinity with n. In 1975 Mignotte [10] obtained a good lower estimate for $|u_n|$ in terms of n when the characteristic polynomial of the recurrence sequence has at most three roots, which are simple, of maximum modulus. It has not yet been established that if $(u_n)_{n=0}^{\infty}$ is a non-degenerate linear recurrence sequence then $P(u_n)$ tends to infinity with n [1]). This is a consequence of the next theorem in the special case that the characteristic polynomial of the sequence has one root of largest modulus.

Theorem 4. *Let K be a field of degree D over $\mathbb{Q}$ and let α be a real algebraic number from K with absolute value greater than one. Let $u(n)$ be an integer which can be written in the form*

$$u(n) = f(n)\,\alpha^n + h(n),$$

where f is a non-zero polynomial with coefficients from K and

$$|h(n)| < |\alpha|^{\delta n}, \tag{7}$$

for some δ with $0 < \delta < 1$. If $f(n)$ and $h(n)$ are non-zero then, for any $\varepsilon > 0$,

$$P\big(u(n)\big) > (1-\varepsilon)\log n, \tag{8}$$

$$Q\big(u(n)\big) > n^{1-\varepsilon}, \tag{9}$$

for n greater than C_9, a number which is effectively computable in terms of ε, δ, α, f, D and the discriminant of K.

The proof of Theorem 4 depends upon a version, due to Waldschmidt [24], of Baker's theorem concerning lower bounds for linear forms in the logarithms of algebraic numbers. The important feature of Waldschmidt's result in this context is the precise dependence in his lower bound on the number of logarithms in the linear form.

For any integer m let $\omega(m)$ denote the number of distinct prime divisors of m. With the hypotheses of Theorem 4 and the additional assumption that

$$\omega\big(u(n)\big) < \frac{\log n}{(\log\log n)^2}$$

we are able to prove by a minor modification of the proof of Theorem 4, see for example Theorem 2. 2 of [21], that for any $\varepsilon > 0$,

$$P\big(u(n)\big) > e^{n^{\left(\frac{1-\varepsilon}{\omega(u(n))}\right)}},$$

for n greater than C_{10}, a number which is effectively computable in terms of ε, δ, α, f, d and the discriminant of K. The above estimate links $P\big(u(n)\big)$ and $\omega\big(u(n)\big)$. Indeed for the proof of Theorem 4 we suppose that $P\big(u(n)\big)$ is less than $\log n$ and we deduce that $\omega\big(u(n)\big)$ is at least $\left(1-\frac{\varepsilon}{2}\right)\frac{\log n}{\log\log n}$. The result then follows from the prime number theorem.

[1]) A. J. van der Poorten announced such a result at the Colloquium on Number Theory of the Janos Bolyai Mathematical Society, July 20—26, 1981, as joint work with J. P. Glass, J. H. Loxton, and H. P. Schlickewei.

A simple application of Theorem 4 yields the following result.

Corollary 1. *Let u_n be the n-th term of a non-degenerate linear recurrence sequence, defined as in* (6), *and assume that* $|\alpha_1|>|\alpha_j|$ *for* $j=2,\dots,t$. *If* $u(n)\neq f_1(n)\alpha_1^n$ *then, for any* $\varepsilon>0$,

$$P(u_n)>(1-\varepsilon)\log n, \qquad Q(u_n)>n^{1-\varepsilon}, \tag{10}$$

for $n>C_{11}$, *a number which is effectively computable in terms of* ε, $\alpha_1,\dots,\alpha_t$ *and* $f_1,\dots,f_t$.

Note that since $|\alpha_1|>|\alpha_j|$ for $j=2,\dots,t$, α_1 is a real number. I. E. Shparlinskij [20], see [12], has proved the estimate (10) for $P(u_n)$ with $(1-\varepsilon)$ replaced by a positive number C_{12} in the case that $f(n)$ is a non-zero constant. In [21] we obtained (8) with $1-\varepsilon$ replaced by C_{13}, a positive number which is effectively computable in terms of α, δ, f and d, and at Oberwolfach in 1977 M. Mignotte [11] observed that such an estimate could be applied to sequences of the form $([\lambda\theta^n])_{n=0}^{\infty}$ and $(\langle\lambda\theta^n\rangle)_{n=0}^{\infty}$ where λ and θ are non-zero real algebraic numbers; for any real number x, $[x]$ denotes the greatest integer less than or equal to x and $\langle x\rangle$ denotes the nearest integer to x. In particular, we have:

Corollary 2. *Let λ and θ be non-zero real algebraic numbers with* $|\theta|>1$. *If* $\lambda\theta^n$ *is not an integer then*

$$P([\lambda\theta^n])>(1-\varepsilon)\log n, \qquad Q([\lambda\theta^n])>n^{1-\varepsilon},$$

for n greater than C_{14}, *a number which is effectively computable in terms of λ and θ only.*

In this connexion we remark that if θ is a real irrational algebraic number, n is a positive integer composed of the primes $q_1,\dots,q_s$ only and ε is any positive real number then

$$P([n\theta])>(1-\varepsilon)\log\log n, \qquad Q([n\theta])>(\log n)^{1-\varepsilon},$$

for n greater than C_{15}, a number which is effectively computable in terms of $q_1,\dots,q_s$ and θ only. The proof of this result is similar to that of Theorem 4.

I would like to thank l'Université de Strasbourg for its hospitality since it was during a visit to l'Université de Strasbourg that this paper was prepared for publication.

2. Preliminary lemmas

Let $\alpha_1,\dots,\alpha_n$ be non-zero algebraic numbers. Put $K=\mathbb{Q}(\alpha_1,\dots,\alpha_n)$ and denote the degree of K over $\mathbb{Q}$ by D. We shall define the height of an algebraic number β to be

$$|a_d|\prod_{i=1}^{d}\max\{1,|\beta_i|\},$$

where $a_dX^d+\dots+a_0=a_d\prod_{i=1}^{d}(X-\beta_i)$ is the minimal polynomial of β in $\mathbb{Z}[X]$. Let $A_1,\dots,A_n$ be upper bounds for the heights of $\alpha_1,\dots,\alpha_n$ respectively and let $b_1,\dots,b_n$ be rational integers with absolute values at most B. We shall assume that $A_1,\dots,A_n$ and B are all at least 3. Let $l_1,\dots,l_n$ be complex numbers satisfying $e^{l_i}=\alpha_i$ for $i=1,\dots,n$ and put

$$\Lambda=b_1l_1+\dots+b_nl_n.$$

For any non-zero complex number z we shall denote the principal branch of the logarithm of z by $\log z$ and for any positive integer m we shall denote $\exp\left(\frac{\log z}{m}\right)$ by $z^{\frac{1}{m}}$. For $j=1,\ldots,n$, put

$$V_j = \max\left\{\log A_j, \frac{|l_j|}{D}\right\}.$$

By choosing indices for the α_i's appropriately we may assume that

$$V_1 \leqq V_2 \leqq \cdots \leqq V_n.$$

Recently Waldschmidt proved the following result.

Lemma 1. *Let q be a prime number such that the field $K\left(\alpha_1^{\frac{1}{q}},\ldots,\alpha_n^{\frac{1}{q}}\right)$ has degree q^n over K. If $\Lambda \neq 0$ then*

$$|\Lambda| > \exp\left(-c^n n^n V_1 \cdots V_n(\log B + \log V_n)\log V_{n-1}\right), \tag{11}$$

where c is a positive number which is effectively computable in terms of D and q only.

Proof. This is Proposition 3. 8 of [24].

Waldschmidt established the above inequality as a step in the proof of a more general result where no hypothesis is made on the degree of $K\left(\alpha_1^{\frac{1}{q}},\ldots,\alpha_n^{\frac{1}{q}}\right)$ over K. However, in removing the condition on the degree of $K\left(\alpha_1^{\frac{1}{q}},\ldots,\alpha_n^{\frac{1}{q}}\right)$ over K he is forced to replace n^n by n^{2n} in the expression on the right hand side of (11). The weaker estimate n^{2n} leads to inequalities like (8) and (9) of Theorem 4 but with $1-\varepsilon$ replaced by $\frac{1}{2}-\varepsilon$. In [14], Loxton and van der Poorten obtained an inequality similar to that of Lemma 1 with a dependence on n of the form $n^{n+o(n)}$ and their result could also be used here. To profitably apply Lemma 1 we shall need, because of the condition on the degree of $K\left(\alpha_1^{\frac{1}{q}},\ldots,\alpha_n^{\frac{1}{q}}\right)$ over K, the following three lemmas which enable us to rework the "final descent" in Waldschmidt's proof of his general result.

Lemma 2. *If $l_1,\ldots,l_n$ are linearly dependent over $\mathbb{Q}$ then there exist rational integers $t_1,\ldots,t_n$, not all zero, such that*

$$t_1 l_1 + \cdots + t_n l_n = 0$$

with

$$|t_k| \leqq (9nD^3)^n \frac{V_1 \cdots V_n}{V_k}.$$

Proof. This is Lemma 4. 1 of [24]. A similar result is Theorem 1 of [15].

Lemma 3. *If $l_1,\ldots,l_n$ are linearly independent over $\mathbb{Q}$ then there exist algebraic numbers $\alpha_1',\ldots,\alpha_n'$ from K with heights at most $A_1',\ldots,A_n'$ respectively and $l_1',\ldots,l_n'$ satisfying $e^{l_j'}=\alpha_j'$ for $j=1,\ldots,n$ such that:*

a) *For each prime number q such that K contains the q-th roots of unity, the field $K\left((\alpha_1')^{\frac{1}{q}},\ldots,(\alpha_n')^{\frac{1}{q}}\right)$ has degree q^n over K.*

b) *For* $1 \leqq s \leqq n$,

$$\max\left\{\frac{\log A'_s}{D}, \frac{|l'_s|}{D}\right\} \leqq V_1 + \cdots + V_s .$$

c) *There exist rational integers* $m_{s,j}$ *with* $1 \leqq s \leqq n$ *and* $0 \leqq j \leqq s$ *such that for* $1 \leqq s \leqq n$,

$$m_{s,0} l_s = \sum_{j=1}^{s} m_{s,j} l'_j ,$$

with $m_{s,0} > 0$, *and*

$$\max_{0 \leqq j \leqq s} |m_{s,j}| \leqq (9 D^3 s^2 V_s)^s .$$

Proof. This is Proposition 4. 3 of [24].

Lemma 4. *Let* q *be a prime number and let* K *be an algebraic number field which contains the* q*-th roots of unity and the non-zero algebraic numbers* $\alpha_1, \ldots, \alpha_n$. *If* $K(\alpha_1^{\frac{1}{q}}, \ldots, \alpha_n^{\frac{1}{q}})$ *has degree less than* q^n *over* K *then for some* γ *in* K *we have*

$$\alpha_1^{r_1} \cdots \alpha_n^{r_n} = \gamma^q ,$$

where $r_1, \ldots, r_n$ *are rational integers, not all zero, with* $0 \leqq r_i \leqq q-1$ *for* $i = 1, \ldots, n$.

Proof. This is Lemma 3 of [2].

Denote by $\wp$ a prime ideal of R, the ring of algebraic integers of K, lying above the rational prime number p and for any non-zero x in K let $\operatorname{ord}_\wp(x)$ denote the exponent of $\wp$ in the canonical decomposition of the fractional ideal generated by x into prime ideals of R. Write $e_\wp$ for the ramification index of $\wp$ and put

$$g = \left[\frac{1}{2} + \frac{e_\wp}{p-1}\right]$$

and

$$G_\wp = (\mathrm{Norm}_{K/Q}\, \wp^g)(\mathrm{Norm}_{K/Q}\, \wp - 1) .$$

In 1976, van der Poorten [13] obtained the following result.

Lemma 5. *If* $\alpha_1^{b_1} \cdots \alpha_n^{b_n} - 1 \neq 0$ *then*

$$\operatorname{ord}_\wp(\alpha_1^{b_1} \cdots \alpha_n^{b_n} - 1) < C \frac{G_\wp}{\log p} \log A_1 \cdots \log A_n (\log B)^2 ,$$

where C *is a positive number which is effectively computable in terms of* n *and* D *only.*

Proof. This is Theorem 2 of [13].

We shall use Lemma 5 in our proof of Theorem 1. Our next result, which gives an estimate for the rate of growth of a non-degenerate binary recurrence sequence, is used in the proofs of Theorem 1 and Theorem 3.

Lemma 6. *Let $u_n = a\alpha^n + b\beta^n$ be the n-th term of a non-degenerate binary recurrence sequence. Then*

$$|u_n| > |\alpha|^{n - C_0 \log n},$$

for $n > C_1$, where C_0 and C_1 are positive numbers which are effectively computable in terms of a and b only.

Proof. This is Lemma 5 of [19] and Lemma 3.2 of [21]. The proof depends upon a result of Baker [1].

Let $(t_n)_{n=0}^{\infty}$ be a Lucas sequence. Since $t_0 = 0$ and $t_1 = 1$ we have from (1),

$$t_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}, \tag{12}$$

for $n \geqq 0$. For the proof of Theorem 2 we require the following result concerning characteristic divisors of Lucas numbers.

Lemma 7. *Let $(t_n)_{n=0}^{\infty}$ be a Lucas sequence, as in* (12). *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*

$$p \geqq l - 1.$$

Proof. We first remark that if p is a prime number which divides $t_2 = \alpha + \beta$ then the result holds. Further, the result applies for $p = 2$ since either 2 divides t_2 or 2 divides $\alpha\beta t_3$. Next, as in Lemma 4 of [22], we observe that if p is a prime number which does not divide $t_2\alpha\beta(\alpha-\beta)^2$ then p divides $t_{p-1}t_{p+1}$ and again our result applies. Finally, as in Lemma 5 of [22], if p is greater than 2 and p divides $(\alpha-\beta)^2$ then p divides t_p. The assumption is made in [22] that $\alpha\beta$ and $\alpha+\beta$ are coprime integers but this assumption is not used in the proofs of the preceding two assertions.

Our final lemma is used in the proof of Theorem 3. For any rational number x let $|x|_p$ denote the p-adic value of x, normalized so that $|p|_p = p^{-1}$.

Lemma 8. *Let $(t_n)_{n=0}^{\infty}$ be a Lucas sequence, as in* (12), *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, for some integer k, $n = kl$ then, for $p > 2$,

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

while for $p = 2$,

$$|t_n|_2 = |t_l|_2 \quad \textit{for } k \textit{ odd},$$

and

$$|t_n|_2 = 2\,|t_{2l}|_2\,|k|_2 \quad \textit{for } k \textit{ even}.$$

Proof. We remark that Lemma 7 assures us that l exists. For any positive integers n and l we have $(t_n, t_l) = t_{(n,l)}$ by Theorem VI of [4]. Thus if p divides t_n then p divides $t_{(n,l)}$ and, by the minimality of l, $(n, l) = l$. Thus l divides n and this proves our first assertion.

If $n = kl$ the lemma follows from Theorem X of [4].

3. The proof of Theorem 1

Recall that $u_n = a\alpha^n + b\beta^n$ for $n \geqq 0$ and $u_n = ru_{n-1} + su_{n-2}$ for $n = 2, 3, \ldots$. Put $(r^2, s) = k$ and for any θ in the ring of algebraic integers of $Q(\alpha)$ let $[\theta]$ denote the ideal generated by θ in that ring. Note that $\frac{\alpha^2}{k}$ and $\frac{\beta^2}{k}$ are the roots of

$$x^2 - \left(\frac{r^2+2s}{k}\right)x + \left(\frac{s}{k}\right)^2$$

and so are algebraic integers in $Q(\alpha)$. Further $\frac{r^2+2s}{k}$ and $\left(\frac{s}{k}\right)^2$ are coprime hence $\left(\left[\frac{\alpha^2}{k}\right], \left[\frac{\beta^2}{k}\right]\right) = [1]$. Put

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

and

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

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

$$P(u_{2n}) \geqq P(v_n), \quad Q(u_{2n}) \geqq Q(v_n), \quad P(u_{2n+1}) \geqq P(w_n) \quad \text{and} \quad Q(u_{2n+1}) \geqq Q(w_n),$$

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 $([\alpha], [\beta]) = [1]$. Further, we may assume that $|\alpha| \geqq |\beta|$. Since α and β are non-zero algebraic integers of degree at most 2 and $\frac{\alpha}{\beta}$ is not a root of unity we have

$$|\alpha| \geqq \sqrt{2}. \tag{15}$$

Let $c_1, c_2, \ldots$ denote positive numbers which are effectively computable in terms of a and b only. From (15) and Lemma 6 we have

$$\log|u_n| > \frac{n}{2}\log|\alpha|, \tag{16}$$

for $n > c_1$. We shall assume henceforth that $n > c_1$.

Let $\wp$ be a prime ideal of the ring of algebraic integers of $Q(\alpha)$ lying above the rational prime number p. For any x in $Q(\alpha)$ let $|x|_{\wp}$ denote the p-adic value of x normalized so that $|x|_{\wp}=p^{-j}$ where $j=\dfrac{\operatorname{ord}_{\wp}x}{\operatorname{ord}_{\wp}p}$. If p divides $\alpha\beta$ then, since $([\alpha],[\beta])=[1]$,

$$|u_n|_{\wp}>p^{-c_2}. \tag{17}$$

On the other hand if p does not divide $\alpha\beta$ then

$$|u_n|_{\wp}=\left|\left(\frac{-a}{b}\right)\left(\frac{\alpha}{\beta}\right)^n-1\right|_{\wp}|b\beta^n|_{\wp},$$

and plainly

$$|b\beta^n|_{\wp}=|b|_{\wp}>p^{-c_3}. \tag{18}$$

We now employ Lemma 5 with $\alpha_1=\dfrac{-a}{b}$, $\alpha_2=\dfrac{\alpha}{\beta}$, $b_1=1$ and $b_2=n$. Since d, the degree of α, is at most 2, $e_{\wp}$ is also at most 2 hence $g=0$ for $p>5$. Thus $G_{\wp}<c_4p^d$ and consequently

$$\left|\left(\frac{-a}{b}\right)\left(\frac{\alpha}{\beta}\right)^n-1\right|_{\wp}>p^{-c_5\frac{p^d}{\log p}\log A(\log n)^2} \tag{19}$$

where A denotes the maximum of 3 and the height of $\dfrac{\alpha}{\beta}$. From (17), (18) and (19) we conclude that

$$\log(|u_n|_p^{-1})<c_6p^d\log A(\log n)^2, \tag{20}$$

for any prime number p. Write

$$|u_n|=p_1^{l_1}\cdots p_r^{l_r},$$

where $p_1,\dots,p_r$ are distinct primes and $l_1,\dots,l_r$ are positive integers. Certainly A is at most $3|\alpha|^2$ and so, by (15), at most $|\alpha|^6$. Thus, from (20),

$$\log|u_n|<c_7\log|\alpha|\,(\log n)^2\left(\sum_{i=1}^{r}p_i^d\right). \tag{21}$$

Comparing (16) and (21) we find

$$c_8\frac{n}{(\log n)^2}<\sum_{i=1}^{r}p_i^d. \tag{22}$$

Put $p_r=P(u_n)$. The right hand side of inequality (22) is at most rp_r^d and so by the prime number theorem

$$c_9\frac{n}{(\log n)^2}<\frac{p_r^{d+1}}{\log p_r}.$$

Thus

$$P(u_n) = p_r > c_{10} \left(\frac{n}{\log n}\right)^{\frac{1}{d+1}},$$

as required. Furthermore,

$$\left(\prod_{i=1}^{r} p_i\right)^d \geqq \sum_{i=1}^{r} p_i^d,$$

and so the desired estimate for $Q(u_n)$ follows from (22).

4. The proof of Theorem 2

Let m be an integer larger than 3 and let p be a characteristic divisor of u_m.

Assume first that p divides $\alpha\beta$. Let $\wp$ be a prime ideal which lies above p in the ring of algebraic integers of $\mathbb{Q}(\alpha)$. If $\wp^{l_1}$ exactly divides $[\alpha]$, the ideal generated by α, and $\wp^{l_2}$ exactly divides $[\beta]$ then one at least of l_1 and l_2 is non-zero. If we assume that both l_1 and l_2 are positive then the recurrence relation

$$u_n = (\alpha+\beta)\, u_{n-1} - \alpha\beta u_{n-2}, \tag{23}$$

for $n = 2, 3, \ldots$, shows that $\wp$, and hence $[p]$, divides $[u_2]$ and $[u_3]$. Since m is greater than 3 we have $u_2 = u_3 = 0$. In this case, however, $(u_n)_{n=0}^{\infty}$ is a degenerate sequence contrary to our assumption. Thus one of l_1 and l_2 is zero, and without loss of generality we may assume that l_2 is zero. Since p is a characteristic divisor of $u_m = a\alpha^m + b\beta^m$ and $m > 3$ we deduce that $\wp$ divides $[(\beta-\alpha)\, b] = [u_1 - u_0\alpha]$ whence $\wp$ divides $[u_1]$. Thus $u_1 = 0$ and by (23) p divides u_2 hence $u_2 = 0$. Again we find that $(u_n)_{n=0}^{\infty}$ is degenerate contrary to our assumption. Therefore p does not divide $\alpha\beta$.

Let $t_n = \dfrac{\alpha^n - \beta^n}{\alpha - \beta}$ be the n-th term of the Lucas sequence associated with $(u_n)_{n=0}^{\infty}$. Since p does not divide $\alpha\beta$ there exists, by Lemma 7, a smallest positive integer l for which p divides t_l, and l satisfies the inequality

$$p \geqq l - 1. \tag{24}$$

If $m < l$ then, by (24),

$$p \geqq m, \tag{25}$$

and (4) holds. Therefore we may assume that $m \geqq l$. We have

$$u_m - a\alpha^{m-l}(\alpha - \beta)\, t_l = \beta^l u_{m-l},$$

and thus, since $a(\alpha-\beta)$ is an algebraic integer and p does not divide $\alpha\beta$, p divides u_{m-l}. But p is a characteristic divisor of u_m so $u_{m-l} = 0$. From Lemma 6, $m - l \leqq C_7 - 1$ whence, from (24),

$$p \geqq m - C_7.$$

This establishes inequality (4).

We shall now assume that $u_m v_m \neq 0$ for $m \geqq 0$. By the preceding paragraph $m < l$ and so

$$a(\alpha-\beta)\, t_l - \alpha^{l-m} u_m = -\beta^m v_{l-m}.$$

Plainly p divides v_{l-m}. Thus

$$p \leqq |b\alpha^{l-m} + a\beta^{l-m}|, \tag{26}$$

since $v_{l-m} \neq 0$. We may assume that $|\alpha| \geqq |\beta|$ hence, from (25) and (26),

$$m \leqq (|a| + |b|)\, |\alpha|^{l-m}.$$

We have $|\alpha| \geqq \sqrt{2}$, as in (15), so

$$\log m < (l-m)\, c_1$$

whence

$$m + c_1^{-1} \log m < l,$$

for a positive number c_1 which is effectively computable in terms of a, b, α and β. The Theorem now follows from (24).

5. The proof of Theorem 3

We may assume, as in the proof of Theorem 1, that $([\alpha], [\beta]) = [1]$ and that $|\alpha| \geqq |\beta|$. To obtain our result we shall assume that there exists a function $\varepsilon(m)$ which tends to zero as m tends to infinity and a positive constant δ such that

$$P(u_m) < \varepsilon(m)\, m \log m, \tag{27}$$

for a set of integers m of positive upper density δ and we shall show that this leads to a contradiction. Plainly we may assume that $\varepsilon(m)$ is strictly decreasing and that $\varepsilon(m) > (\log m)^{-1}$ for $m > 1$. Accordingly, we can find arbitrarily large integers n such that between n and $2n$ there are at least $\frac{\delta n}{2}$ integers m which satisfy (27).

Put $T = \varepsilon(n)\, 2n \log 2n$ and for each prime p less than T let $u_{m(p)}$ be the term with $n \leqq m(p) \leqq 2n$ 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 $u_{m(p)}$. For n sufficiently large $\varepsilon(n)$ is less than $\frac{\delta}{10}$ and by the prime number theorem there are at most $\frac{\delta n}{3}$ integers of the form $m(p)$. Denote by M the set of those integers m between n and $2n$ which are not associated with a prime p less than T and for which (27) holds. Plainly M has at least $\frac{\delta n}{6}$ members. To obtain a contradiction we compare estimates for $\left|\prod_{m \in M} u_m\right|$.

We first estimate the product from below. From Lemma 6 $|u_m| > |\alpha|^{m - C_0 \log m}$, where C_0 is a positive number which is effectively computable in terms of a and b only. For n sufficiently large, $m - C_0 \log m > \frac{n}{2}$ and thus

$$(28) \qquad |\prod_{m \in M} u_m| > |\alpha|^{\frac{\delta n^2}{12}}.$$

Alternatively, we can prove, in an elementary way, that at most three integers m with $n \leqq m \leqq 2n$ satisfy

$$|u_m| < |\alpha|^{\frac{3}{4}m},$$

and then estimate (28) again follows. This approach has the virtue that the proof becomes completely elementary. Accordingly, assume that $|u_{n_i}| < |\alpha|^{\frac{3}{4}n_i}$ for integers n_1 and n_2 with $n_1 > n_2 \geqq n$. Certainly $|\alpha| = |\beta|$ in this case. Then

$$\left|\left(\frac{\alpha}{\beta}\right)^{n_i} + \frac{b}{a}\right| < |a|^{-1} |\beta|^{-\frac{1}{4}n_i},$$

for i equal to 1 and 2. Thus

$$\left|\left(\frac{\alpha}{\beta}\right)^{n_1} - \left(\frac{\alpha}{\beta}\right)^{n_2}\right| < 2|a|^{-1} |\beta|^{-\frac{1}{4}n_2},$$

and so

$$|\alpha^{n_1 - n_2} - \beta^{n_1 - n_2}| < 2|a|^{-1} |\beta|^{n_1 - \frac{5}{4}n_2}.$$

Since the left-hand side of the above inequality is at least 1 we see that $n_1 > \frac{6}{5} n_2$ for n sufficiently large and since $\left(\frac{6}{5}\right)^4 > 2$ this establishes our claim.

We next estimate the product from above. Put

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

Clearly

$$(29) \qquad |\prod_{m \in M} u_m| \leqq \prod_{p < T} |S(p)|_p^{-1},$$

and for our purpose it will be sufficient to estimate $|S(p)|_p$ for p less than T.

We first estimate $|S(p)|_p$ for those primes p which divide $\alpha\beta$. Let $\wp$ be a prime ideal divisor of $[p]$ with ramification index $e_\wp$. Then $\wp$ divides either $[\alpha]$ or $[\beta]$ and we shall assume, without loss of generality, that $\wp$ divides $[\alpha]$. Put $a' = (\beta - \alpha)\, a$ and $b' = (\beta - \alpha)\, b$. If $[p]^l$, hence also $\wp^{e_\wp l}$, exactly divides $[u_m]$ it exactly divides $[b']$ for m sufficiently large. Thus

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

whence

$$\prod_{\substack{p<T \\ p\mid\alpha\beta}} |S(p)|_p^{-1} \leqq \prod_{\substack{p<T \\ p\mid\alpha\beta}} |a'b'|_p^{-n}. \tag{30}$$

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

$$u_m - \beta^r u_{m-r} = a' \alpha^{m-r} t_r. \tag{31}$$

On setting $m = m(p)$ in (31) and letting r run over those integers such that $m(p) - r \geqq n$ we find that

$$|u_{m(p)-1} \cdots u_n|_p \geqq \prod_{r=1}^{m(p)-n} (|t_r|_p \, |a'b'|_p). \tag{32}$$

Let l be the smallest integer for which p divides t_l; l exists by Lemma 7. By Lemma 8, if $p > 2$ then

$$\prod_{r=1}^{m(p)-n} |t_r|_p = |t_l|_p^{s_1} \, |s_1!|_p, \tag{33}$$

where $s_1 = \left[\dfrac{m(p)-n}{l}\right]$, while if $p = 2$

$$\prod_{r=1}^{m(p)-n} |t_r|_2 = |t_l|_2^{s_1} \left|\frac{t_{2l}}{t_l}\right|_2^{s_2} |s_2!|_2, \tag{34}$$

where $s_2 = \left[\dfrac{m(p)-n}{2l}\right]$. Similarly on setting $m - r = m(p)$ in (31) and letting r run over those integers such that $m(p) + r \leqq 2n$ we find that for $p > 2$

$$|u_{m(p)+1} \cdots u_{2n}|_p \geqq |t_l|_p^{s_3} \, |s_3!|_p \, |a'b'|_p^{2n-m(p)}, \tag{35}$$

while for $p = 2$,

$$|u_{m(p)+1} \cdots u_{2n}|_2 \geqq |t_l|_2^{s_3} \left|\frac{t_{2l}}{t_l}\right|_2^{s_4} |s_4!|_2 \, |a'b'|_2^{2n-m(p)}, \tag{36}$$

where $s_3 = \left[\dfrac{2n-m(p)}{l}\right]$ and $s_4 = \left[\dfrac{2n-m(p)}{2l}\right]$. Thus, from (32), (33) and (35), we see that if p is a prime number which does not divide $2\alpha\beta$ then

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

where $s = \left[\dfrac{n}{l}\right]$ and therefore, since $|t_l| \leqq 2|\alpha|^l$,

$$|S(p)|_p^{-1} \leqq (2|\alpha|)^n |n!|_p^{-1} |a'b'|_p^{-n}. \tag{37}$$

From, (32), (34) and (36),

$$|S(2)|_2^{-1} \leqq |t_l|^s \left|\frac{t_{2l}}{t_l}\right|^s |s!|_2^{-1} |a'b'|_2^{-n} \leqq (2|\alpha|)^{2n} |n!|_2^{-1} |a'b'|_2^{-n}. \tag{38}$$

Thus, from (30), (37) and (38),

$$\prod_{p<T} |S(p)|_p^{-1} \leqq \prod_{p<T} \left((2|\alpha|)^{2n} |n!|_p^{-1} |a'b'|_p^{-n}\right). \tag{39}$$

Further, we have

$$\prod_{p<T} \left(|n!|_p^{-1} |a'b'|_p^{-n}\right) \leqq n^n |a'b'|^n. \tag{40}$$

Since $\varepsilon(n) > (\log n)^{-1}$ and $T = \varepsilon(n)\, 2n \log 2n$ it follows from the prime number theorem, (39), and (40), that

$$\prod_{p<T} |S(p)|_p^{-1} \leqq (2|\alpha|)^{\varepsilon(n) 6n^2} n^n |a'b'|^n, \tag{41}$$

for n sufficiently large. We have $|\alpha| \geqq \sqrt{2}$ since $|\alpha| \geqq |\beta|$ and $(u_n)_{n=0}^{\infty}$ is non-degenerate. Thus, from (29) and (41),

$$\left|\prod_{m \in M} u_m\right| \leqq |\alpha|^{\varepsilon(n) 20 n^2}.$$

Comparing the estimate with (28) we obtain a contradiction for n sufficiently large. This establishes the theorem.

6. The proof of Theorem 4

We may assume, by replacing $f(n)$ by $-f(n)$ if necessary, that α is a positive real number. Further, we shall suppose throughout that n exceeds a sufficiently large number c_1; here $c_1, c_2, \ldots$ are positive numbers which are effectively computable in terms of ε, δ, α, f, D and the discriminant of K.

The proof proceeds by a comparison of estimates for $|\log R|$, where

$$R = \frac{u(n)}{f(n)\, \alpha^n}. \tag{42}$$

We have $R = 1 + \dfrac{h(n)}{f(n)\, \alpha^n}$ and for n sufficiently large

$$|\log R| \leqq \frac{2|h(n)|}{|f(n)|\, \alpha^n},$$

since for any real number x with $|x| < \dfrac{1}{2}$ we have $|\log(1+x)| \leqq 2|x|$. Thus, from (7),

$$|\log R| \leqq \alpha^{-\frac{(1-\delta)n}{2}}. \tag{43}$$

We shall now derive a lower bound for $|\log R|$ with the aid of Lemmas 1, 2, 3 and 4. Let a and b be the smallest positive integers, such that $af(n)$ and $b\alpha$ are algebraic integers and denote by $q_1, \ldots, q_s$ the prime numbers which divide either a, b, $\mathrm{Norm}_{K/\mathbb{Q}}(b\alpha)$ or the discriminant of K. Note that s is less than c_2. Write

$$u(n) = p_1^{b_1} \cdots p_t^{b_t} q_1^{a_1} \cdots q_s^{a_s}, \tag{44}$$

where $a_1, \ldots, a_s$ are non-negative integers, $b_1, \ldots, b_t$ are positive integers and $p_1, \ldots, p_t$ are distinct prime numbers different from $q_1, \ldots, q_s$. Put

$$af(n) = p_1^{d_1} \cdots p_t^{d_t} f_1(n), \tag{45}$$

where $d_1, \ldots, d_t$ are non-negative integers which are chosen as large as possible subject to the restriction that $f_1(n)$ is an algebraic integer. Note that $d_i < c_3 \log n$ for $i = 1, \ldots, t$. Put $k_i = b_i - d_i$ for $1, \ldots, t$ and, by reindexing the q_i's if necessary, write

$$a_1 \log q_1 + \cdots + a_s \log q_s + \log a = k_{t+1} \log q_1 + \cdots + k_{t+r} \log q_r, \tag{46}$$

where $k_{t+1}, \ldots, k_{t+r}$ are positive integers and $r \leqq s$. Since α is a positive real number we have $\log(\alpha^n) = n \log \alpha$ and thus, from (42), (44) and (46),

(47)

$$\log R = k_1 \log p_1 + \cdots + k_t \log p_t + k_{t+1} \log q_1 + \cdots + k_{t+r} \log q_r - \log f_1(n) - n \log \alpha.$$

We remark that $|k_i| \leqq c_4 n$ for $i = 1, \ldots, t+r$.

Assume now that $\log q_1, \ldots, \log q_r$, $\log \alpha$ and $\log f_1(n)$ are linearly independent over $\mathbb{Q}$ and put $\alpha_1 = q_1, \ldots, \alpha_r = q_r$, $\alpha_{r+1} = \alpha$ and $\alpha_{r+2} = f_1(n)$. By Lemma 3 there exist numbers $\alpha'_1, \ldots, \alpha'_{r+2}$ from K with heights at most $A'_1, \ldots, A'_{r+2}$ respectively, $l'_1, \ldots, l'_{r+2}$ satisfying $e^{l'_j} = \alpha'_j$ for $j = 1, \ldots, r+2$ and rational integers $m_{i,j}$ with $1 \leqq i \leqq r+2$ and $0 \leqq j \leqq i$ such that for $1 \leqq i \leqq r+2$, $m_{i,0} > 0$,

$$m_{i,0} \log \alpha_i = \sum_{j=1}^{i} m_{i,j} l'_j, \tag{48}$$

and

$$\max_{0 \leqq j \leqq i} |m_{i,j}| \leqq (\log n)^{c_5}.$$

Further, $K(\sqrt{\alpha'_1}, \ldots, \sqrt{\alpha'_{r+2}})$ has degree 2^{r+2} over K and if we put

$$V'_j = \max\left\{\log A'_j, \frac{|l'_j|}{D}\right\}$$

then

$$V'_j < c_6, \tag{49}$$

for $j = 1, \ldots, r+1$ and

$$V'_{r+2} < c_7 \log n. \tag{50}$$

Therefore, from (47) and (48),

$$m_{1,0} \cdots m_{r+2,0} \log R = g_1 \log p_1 + \cdots + g_t \log p_t + g_{t+1} l'_1 + \cdots + g_{t+r+2} l'_{r+2},$$

where

$$|m_{1,0} \cdots m_{r+2,0}| < (\log n)^{c_8},$$

and

$$\max_{1 \leqq i \leqq t+r+2} |g_i| < n(\log n)^{c_9}. \tag{51}$$

We shall now show that $K(\sqrt{p_1}, \ldots, \sqrt{p_t}, \sqrt{\alpha'_1}, \ldots, \sqrt{\alpha'_{r+2}})$ has degree 2^{t+r+2} over K. If it does not then by Lemma 4 there exist integers $z_1, \ldots, z_{t+r+2}$, not all zero, with $0 \leqq z_i < 2$ for $i = 1, \ldots, t+r+2$ such that

$$p_1^{z_1} \cdots p_t^{z_t} (\alpha'_1)^{z_{t+1}} \cdots (\alpha'_{r+2})^{z_{t+r+2}} = \gamma^2 \tag{52}$$

for some algebraic number γ in K. We shall show first that $z_i = 0$ for $i = 1, \ldots, t$. Write

$$[p_i] = \wp_1^{e_1} \cdots \wp_v^{e_v},$$

where $\wp_1, \ldots, \wp_v$ are distinct prime ideals of the ring of algebraic integers of K and $e_1, \ldots, e_v$ are positive integers. Indeed $e_1 = \cdots = e_v = 1$ since p_i does not divide the discriminant of K. By our choice of d_i, recall (45), there is some prime ideal $\wp_l$ which does not divide $[f_1(n)]$. From (48), we have

$$\alpha_i^{m_{i,0}} = \prod_{j=1}^{i} (\alpha'_j)^{m_{i,j}}, \tag{53}$$

with $m_{i,0} > 0$ for $i = 1, \ldots, r+2$. Arguing inductively from (53) we find that $\wp_l$ does not occur in the canonical decomposition of the fractional ideal generated by α'_j for $j = 1, \ldots, r+2$. Thus, from (52), $\mathrm{ord}_{\wp_l}(\gamma^2) = z_i$. Since $\mathrm{ord}_{\wp_l}(\gamma^2) = 2\,\mathrm{ord}_{\wp_l}(\gamma)$ and $0 \leqq z_i < 2$ we conclude that $z_i = 0$ for $i = 1, \ldots, t$. Thus we have

$$(\alpha'_1)^{z_{t+1}} \cdots (\alpha'_{r+2})^{z_{t+r+2}} = \gamma^2,$$

with $z_{t+1}, \ldots, z_{t+r+2}$ not all zero, hence the degree of $K(\sqrt{\alpha'_1}, \ldots, \sqrt{\alpha'_{r+2}})$ over K is less than 2^{r+2} and this is a contradiction. Therefore, $K(\sqrt{p_1}, \ldots, \sqrt{p_t}, \sqrt{\alpha'_1}, \ldots, \sqrt{\alpha'_{r+2}})$ has degree 2^{t+r+2} over K.

If, on the other hand, $\log q_1, \ldots, \log q_r$, $\log \alpha$ and $\log f_1(n)$ are linearly dependent over Q then, by Lemma 2, there exist integers $h_1, \ldots, h_{r+2}$, not all zero, such that

$$h_1 \log q_1 + \cdots + h_r \log q_r + h_{r+1} \log \alpha + h_{r+2} \log f_1(n) = 0, \tag{54}$$

with $\max_{1 \leqq i \leqq r+2} |h_i| < c_{10} \log n$. One of h_{r+1} and h_{r+2} is non-zero since $\log q_1, \ldots, \log q_r$ are linearly independent over Q. If h_{r+1} is non-zero then, from (47) and (54),

$$h_{r+1} \log R = k'_1 \log p_1 + \cdots + k'_t \log p_t + k'_{t+1} \log q_1 + \cdots + k'_{t+r} \log q_r + k'_{t+r+1} \log f_1(n),$$

with $|k'_i| \leqq c_{11} n \log n$ for $i = 1, \ldots, t+r+1$. In a similar fashion if h_{r+2} is non-zero we can express $h_{r+2} \log R$ as a linear combination of $\log p_1, \ldots, \log p_t$, $\log q_1, \ldots, \log q_r$ and $\log \alpha$ with integer coefficients less than $c_{12} n \log n$ in absolute value. If in the former case $\log q_1, \ldots, \log q_r$ and $\log f_1(n)$ are linearly dependent, or in the latter case $\log q_1, \ldots, \log q_r$ and $\log \alpha$ are linearly independent, then a second application of Lemma 2 shows that for some non-zero integer M_0 with $|M_0| < c_{13} (\log n)^2$ we have

$$M_0 \log R = k''_1 \log p_1 + \cdots + k''_t \log p_{t+r} + k''_{t+1} \log q_1 + \cdots + k''_{t+r} \log q_r,$$

with $|k_i''| < c_{14} n (\log n)^2$. Therefore, after at most two applications of Lemma 2, we produce a non-zero multiple of $\log R$ which is expressed as a linear combination of logarithms which are linearly independent over $\mathbb{Q}$. We may now employ Lemmas 3 and 4 as we did in the preceding two paragraphs to obtain a non-zero multiple of $\log R$ which is expressed as a linear combination of logarithms of algebraic numbers, the square roots of which generate a field of maximal degree over K.

Thus, whether $\log q_1, \dots, \log q_s$, $\log \alpha$ and $\log f_1(n)$ are linearly independent over $\mathbb{Q}$ or not, there exist, for y equal to r, $r+1$ or $r+2$, algebraic numbers $\alpha_1'', \dots, \alpha_y''$ with heights $A_1'', \dots, A_y''$ respectively, some non-zero integer M with

$$(55) \qquad |M| < (\log n)^{c_{15}},$$

$l_1'', \dots, l_y''$ such that $e^{l_j''} = \alpha_j''$ for $j = 1, \dots, y$, and integers $w_1, \dots, w_{t+y}$ such that

$$(56) \qquad M \log R = w_1 \log p_1 + \cdots + w_t \log p_t + w_{t+1} l_1'' + \cdots + w_{t+y} l_y'',$$

and such that $K(\sqrt{p_1}, \dots, \sqrt{p_t}, \sqrt{\alpha_1''}, \dots, \sqrt{\alpha_y''})$ has degree 2^{t+y} over K. Further, as in (51),

$$(57) \qquad \max_{1 \leq i \leq t+y} |w_i| < n (\log n)^{c_{16}}$$

and if we put

$$V_j'' = \max\left\{A_j'', \frac{|l_j''|}{D}\right\},$$

for $j = 1, \dots, y$ then, as in (49) and (50),

$$(58) \qquad V_j'' < c_{17},$$

for $j = 1, \dots, y-1$, and

$$(59) \qquad V_y'' < c_{18} \log n.$$

We may now use Lemma 1 with $q = 2$ to estimate $|M \log R|$ from below. We remark that $M \log R \neq 0$ since M and $h(n)$ are non-zero. Further we may assume that $p_t \leq n$, where $p_t = \max\limits_{1 \leq i \leq t} \{p_i\}$, for otherwise the theorem holds. From (56), (57), (58), (59) and Lemma 1 we find

$$(60) \qquad \log |M \log R| > -c_{19}^m m^m \log p_1 \cdots \log p_t (\log n)^3,$$

where $m = t + y$. By contrast, it follows from (43) and (55) that

$$(61) \qquad \log |M \log R| < -c_{20} n,$$

for n sufficiently large, and a comparison of (60) and (61) reveals that

$$(62) \qquad \log n - 3 \log \log n - c_{21} < c_{22} m + m \log m + \log \log p_1 + \cdots + \log \log p_t.$$

Certainly the left hand side of inequality (62) is at least $\left(1-\frac{\varepsilon}{10}\right)\log n$ for n sufficiently large and thus, since we may assume that $0<\varepsilon<1$, m is at least $c_{23}\sqrt{\log n}$. Since $m=t+y$ and $y<c_{24}$ we deduce that

$$(63)\qquad \left(1-\frac{\varepsilon}{10}\right)\log n<\left(1+\frac{\varepsilon}{10}\right)t\log t+\log\log p_1+\cdots+\log\log p_t,$$

for n sufficiently large. By the arithmetic-geometric mean inequality

$$\prod_{i=1}^{t}\log p_i\leqq\left(\frac{\log\left(\prod_{i=1}^{t}p_i\right)}{t}\right)^t.$$

Since $\prod_{i=1}^{t}p_i\leqq Q(u(n))$, it follows from (63) that

$$\left(1-\frac{\varepsilon}{10}\right)\log n<\frac{\varepsilon}{10}t\log t+t\log\log Q(u(n)).$$

If we assume that t is less than $\left(1-\frac{\varepsilon}{5}\right)\frac{\log n}{\log\log n}$ then $t\log t$ is less than $\log n$ hence

$$\left(1-\frac{\varepsilon}{5}\right)\log n<t\log\log Q(u(n)),$$

from which it follows that $Q(u(n))>n$, as required. Thus we may assume that t is at least $\left(1-\frac{\varepsilon}{5}\right)\frac{\log n}{\log\log n}$ and in this case the product of the first t primes is at least $n^{1-\varepsilon}$ for n sufficiently large. Therefore,

$$Q(u(n))\geqq\prod_{i=1}^{t}p_i>n^{1-\varepsilon},$$

and this establishes (9).

For the proof of (8) we may assume that p_t is less than $\log n$. As a consequence the right-hand side of (63) is less than $\left(1+\frac{\varepsilon}{5}\right)t\log t$, whence $\left(1-\frac{\varepsilon}{3}\right)\log n<t\log t$, for n sufficiently large. Thus

$$t>\left(1-\frac{\varepsilon}{3}\right)\frac{\log n}{\log\log n}.$$

Certainly p_t is greater than or equal to the t-th prime number and so by the prime number theorem

$$p_t>(1-\varepsilon)\log n,$$

for n sufficiently large. Since $P(u(n))\geqq p_t$, this completes the proof of the theorem.

References

[1] *A. Baker*, A sharpening of the bounds for linear forms in logarithms. II, Acta Arith. **24** (1973), 33—36.
[2] *A. Baker* and *H. M. Stark*, On a fundamental inequality in number theory, Annals of Math. **94** (1971), 190—199.
[3] *G. D. Birkhoff* and *H. S. Vandiver*, On the integral divisors of $a^n - b^n$, Annals of Math. (2) **5** (1904), 173—180.
[4] *R. D. Carmichael*, On the numerical factors of the arithmetic forms $\alpha^n \pm \beta^n$, Annals of Math. (2) **15** (1913), 30—70.
[5] *G. H. Hardy* and *E. M. Wright*, An introduction to the theory of numbers, 4th ed., Oxford 1960.
[6] *D. J. Lewis*, Diophantine equations: p-adic methods, Studies in number theory **6**, ed. W. J. Leveque, Englewood Cliffs, New Jersey, 1969.
[7] *K. Mahler*, Eine arithmetische Eigenschaft der rekurrierenden Reihen, Mathematica (Leiden) **3** (1934—35), 153—156.
[8] *K. Mahler*, Eine arithmetische Eigenschaft der Taylor-Koeffizienten rationaler Funktionen, Proc. Akad. Wetensch. Amsterdam **38** (1935), 50—60.
[9] *K. Mahler*, A remark on recursive sequences, J. Math. Sci. **1** (1966), 12—17.
[10] *M. Mignotte*, A note on linear recursive sequences, J. Austral. Math. Soc. (A) **20**, (1975), 242—244.
[11] *M. Mignotte*, Tagungsbericht Math. Inst., Oberwolfach 1977.
[12] *Št. Porubsky*, Review 10003, Zentralblatt für Math. **437** (1981).
[13] *A. J. van der Poorten*, Linear forms in logarithms in the p-adic case, in Transcendence theory: advances and applications, A. Baker and D. W. Masser ed., London and New York 1977.
[14] *A. J. van der Poorten* and *J. H. Loxton*, Computing the effectively computable bounds in Baker's inequality for linear forms in logarithms, Bull. Austral. Math. Soc. **15** (1976), 33—57 and **17** (1977), 151—155.
[15] *A. J. van der Poorten* and *J. H. Loxton*, Multiplicative relations in number fields, Bull. Austral. Math. Soc. **16** (1977), 83—98 and **17** (1977), 151—155.
[16] *A. Schinzel*, On two theorems of Gelfond and some of their applications, Acta Arith. **13** (1967), 177—236.
[17] *A. Schinzel*, Primitive divisors of the expression $A^n - B^n$ in algebraic number fields, J. reine angew. Math. **268/269** (1974), 27—33.
[18] *T. N. Shorey* and *C. L. Stewart*, On divisors of Fermat, Fibonacci, Lucas and Lehmer numbers. II, J. London Math. Soc. (2) **23** (1981), 17—23.
[19] *T. N. Shorey* and *C. L. Stewart*, On the Diophantine equation $ax^{2t} + bx^t y + cy^2 = d$ and pure powers in recurrence sequences, Math. Scand., to appear.
[20] *I. E. Shparlinskij*, Prime divisors of recurrent sequences, Isv. Vyssh. Uchebn. Zaved. Mat. (4) **215** (1980), 101—103.
[21] *C. L. Stewart*, Divisor properties of arithmetical sequences, Ph. D. Thesis, Cambridge 1976.
[22] *C. L. Stewart*, On divisors of Fermat, Fibonacci, Lucas and Lehmer numbers, Proc. London Math. Soc. (3) **35** (1977), 425—447.
[23] *C. L. Stewart*, Primitive divisors of Lucas and Lehmer numbers, in Transcendence theory: advances and applications, A. Baker and D. W. Masser ed., London and New York 1977.
[24] *M. Waldschmidt*, A lower bound for linear forms in logarithms, Acta Arith. **37** (1980), 257—283.
[25] *M. Ward*, Prime divisors of second order recurring sequences, Duke Math. J. **21** (1954), 607—614.
[26] *K. Zsigmondy*, Zur Theorie der Potenzreste, Monatsh. Math. **3** (1892), 265—284.

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

Eingegangen 18. Juli 1981