MATH. SCAND. 52 (1983), 24–36

ON THE DIOPHANTINE EQUATION $ax^{2t}+bx^ty+cy^2=d$ AND PURE POWERS IN RECURRENCE SEQUENCES

T. N. SHOREY AND C. L. STEWART*

1. Introduction.

Let a, b, c, and d be integers with d non-zero and b^2-4ac positive and not a perfect square. Gauss proved that if the equation

$$ax^2+bxy+cy^2 = d\,, \tag{1}$$

has one solution in integers x and y then the equation has infinitely many solutions in integers x and y. If in (1) we replace x by x^t with t an integer larger than one then the situation changes. In this case we are able to prove:

THEOREM 1. *Let a, b, c, and d be integers with b^2-4ac and acd non-zero. If x, y and t are integers with $|x|$ and t larger than one satisfying*

$$ax^{2t}+bx^ty+cy^2 = d\,,$$

then the maximum of $|x|$, $|y|$ and t is less than C, a number which is effectively computable in terms of a, b, c and d.

Our next theorem asserts that any non-degenerate binary recurrence sequence contains only finitely many terms which are pure powers; a result of this character is required for the proof of Theorem 1. Shorey and Tijdeman [12] proved that there are only finitely many pure powers in the Lucas sequence defined by $u_0=0$, $u_1=1$, and $u_n=(x+1)u_{n-1}+xu_{n-2}$ for $n\geqq 2$, where x is a fixed integer larger than one. In the special case of the Fibonacci sequence defined by $u_0=0$, $u_1=1$, and $u_n=u_{n-1}+u_{n-2}$ for $n\geqq 2$, Cohn [4] and Wyler [14] proved that the nth term is a square only when $n=0$, 1, 2 or 12. Cohn [6] applied this result and a related result [5] to determine all solutions of several Diophantine equations.

* This research was supported in part by a grant from the Natural Sciences and Engineering Research Council of Canada.

Received September 25, 1981; in revised form December 14, 1981.

Let r_1 and r_2 be integers with $r_1^2+4r_2$ non-zero. Let u_0 and u_1 be integers and put

$$u_n = r_1 u_{n-1} + r_2 u_{n-2}, \qquad \text{for } n = 2, 3, \ldots .$$

Then for $n \geqq 0$ we have

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

where α and β are the two roots of $x^2 - r_1 x - r_2$ and

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

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

THEOREM 2. *Let d be a non-zero integer and let u_n, defined as in* (2), *be the n-th term of a non-degenerate binary recurrence sequence. If*

$$dx^q = u_n,$$

for integers x and q larger than one, then the maximum of x, q and n is less than C, a number which is effectively computable in terms of a, α, b, β and d.

Since $(u_n)_{n=0}^\infty$ is a non-degenerate sequence it follows, see Lemma 5, that $|u_n| \to \infty$ as $n \to \infty$ and so, from Theorem 2, u_n is a pure power for only finitely many integers n.

We are able to show that u_n, the nth term of a non-degenerate general recurrence sequence, cannot be a qth power for q sufficiently large, if the characteristic polynomial of u_n has a unique root of largest absolute value. Let $r_1, r_2, \ldots, r_k$ and $u_0, \ldots, u_{k-1}$ be integers with $r_k \neq 0$. Put

$$u_n = r_1 u_{n-1} + \ldots + r_k u_{n-k}, \qquad \text{for } n = k, k+1, \ldots .$$

Let $\alpha_1, \ldots, \alpha_t$ be the distinct roots of the characteristic polynomial $x^k - r_1 x^{k-1} - \ldots - r_k$ of the recurrence sequence. If α_1 has multiplicity one then for $n \geqq 0$ we have

$$u_n = a_1\alpha_1^n + P_2(n)\alpha_2^n + \ldots + P_t(n)\alpha_t^n, \tag{3}$$

where $P_i(n)$ is a polynomial with degree less than the multiplicity of α_i in the characteristic polynomial of u_n, and where a_1 and the coefficients of $P_2(n), \ldots, P_t(n)$ are numbers from the field $Q(\alpha_1, \ldots, \alpha_n)$. (Here Q denotes the field of rational numbers.)

THEOREM 3. *Let d be a non-zero integer and let u_n satisfy* (3). *If $|\alpha_1| > |\alpha_j|$ for $j = 2, \ldots, t, a_1$ and $u_n - a_1\alpha_1^n$ are non-zero and*

$$dx^q = u_n ,$$

for integers and x and q larger than one, then q is less than C, a number which is effectively computable in terms of $d, \alpha_1, \ldots, \alpha_k, a_1$ and the coefficients and degrees of $P_2, \ldots, P_t$.

We are able to show that certain ternary recurrence sequences can be pure powers only finitely many times. In proving our final theorem concerning simultaneous solutions of quadratic equations we are led to consider the equation

$$z^q = a_1\alpha^{2n} + a_2\alpha^{-2n} + a_3 , \tag{4}$$

where α is a real quadratic irrational number and a_1, a_2, and a_3 are non-zero numbers from the field $Q(\alpha)$. We show that equation (4) has only finitely many solutions in integers z, q and n all larger than one provided that $a_2^2 \neq 4a_1a_3$.

THEOREM 4. *Let a, b, c, d, a_1, b_1, c_1, and d_1 be integers with a, c, d, a_1, c_1, and d_1 non-zero. Assume the simultaneous equations*

$$a_1x^2 + b_1xy + c_1y^2 = d_1 , \tag{5}$$

$$ax^2 + bxy + cy^2 = dz^q , \tag{6}$$

have solutions in integers x, y, z, and q with $|z|$ and q larger than one. Let α_1 and α_2 be the roots of $a_1x^2 + b_1x + c_1$. If α_1 and α_2 are not roots of $ax^2 + bx + c$, $b_1^2 \neq 4a_1c_1$, and $b^2 \neq 4ac$, then the maximum of $|x|$, $|y|$, $|z|$ and q is less than C, a number which is effectively computable in terms of a, b, c, d, a_1, b_1, c_1 and d_1.

In his book on Diophantine equations, Mordell, [9], remarks that the simultaneous equations (5) and (6) have only finitely many solutions in integers x, y, and z, if q is fixed as two, $b_1^2 \neq 4a_1c_1$, $b^2 \neq 4ac$, and the roots of $a_1x^2 + b_1x + c_1$ are different from those of $ax^2 + bx + c$. Mordell observed that the solutions x and y must occur as the solutions of a finite number of binary quartic forms and by a result of Thue they are finite in number.

2. Preliminary lemmas.

Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be non-zero algebraic numbers. Let $K = Q(\alpha_1, \ldots, \alpha_n)$ and denote the degree of K over Q by D. Let $A_1, \ldots, A_n$ be upper bounds for the heights of $\alpha_1, \ldots, \alpha_n$, respectively; the height of an algebraic number is the maximum of the absolute values of the relatively prime integer coefficients in its minimal polynomial. We assume that A_n is at least 4. Further let $b_1,\dots,b_{n-1}$ be rational integers with absolute values at most B, and let b_n be a non-zero rational integer with absolute value at most B'. We assume that B' is at least three. Put

$$\Lambda = b_1 \log \alpha_1 + \dots + b_n \log \alpha_n ,$$

where the logarithms are assumed to have their principal values. In 1973 Baker proved the following result; take $\delta = 1/B'$, in Theorem 1 of [1].

LEMMA 1. *If $\Lambda \neq 0$, then $|\Lambda| > \exp(-C(\log B' \log A_n + B/B'))$, where C is a positive number which is effectively computable in terms of n, D and $A_1,\dots,A_{n-1}$ only.*

In 1976 van der Poorten established the following p-adic analogue of Baker's theorem; take $\delta = 1$ in Theorem 3 of [10].

LEMMA 2. *Let $\mathfrak{p}$ be a prime ideal of K lying above the rational prime p and assume that b_n is not divisible by p. If $\alpha_1^{b_1}\dots\alpha_n^{b_n}-1$ is non-zero, then*

$$\operatorname{ord}_{\mathfrak{p}}(\alpha_1^{b_1}\dots\alpha_n^{b_n}-1) < C\left(\log B' \log A_n + \frac{B}{B'}\right),$$

where C is a positive number which is effectively computable in terms of $n, D, A_1,\dots,A_{n-1}$ and p only.

The next result which we shall state was established by S. V. Kotov [7] in 1976.

LEMMA 3. *Let K be an algebraic number field of degree d over the rationals, and let m and n be distinct integers with $m \geqq 2$ and $n \geqq 3$. Put $G(x,y) = \alpha x^m + \beta y^n$, where α and β are non-zero algebraic integers from K. If x and y are coprime algebraic integers from K, and the greatest prime factor of* Norm $(G(x,y))$ *is less than C, then* max $\{|\text{Norm}\,(x)|, |\text{Norm}\,(y)|\}$ *is less than C_1, a number which is effectively computable in terms of C and the parameters of G and K.*

We shall also require the following result, due to Baker, which gives bounds for the solutions of the hyperelliptic equation. Let x be in an algebraic number field K. We denote by $\|x\|$ the maximum of the absolute value of the conjugates of x.

LEMMA 4. *Let K be an algebraic number field of degree d over the rationals Let $a_n \neq 0, a_{n-1},\dots,a_0$ and b be algebraic numbers from K, and let m and n be* *positive integers with* $m \geqq 2$. *Further let* $f(x) = a_n x^n + \ldots + a_1 x + a_0$ *be a polynomial with at least* 3 *simple roots. All solutions in algebraic integers* x, y *from* K *of the Diophantine equation*

$$by^m = f(x),$$

satisfy $\max\{\|x\|, \|y\|\} < C$, *where* C *is a number which is effectively computable in terms of* $b, a_0, a_1, \ldots, a_n$ *and the parameters of* K.

Proof. When K is the field of rational numbers the result follows from Theorems 1 and 2 of [2]. The generalization to an algebraic number field K follows directly as is indicated by Theorem 4.1 and 4.2 of [3].

We require an estimate from below for the absolute value of u_n the nth term of a non-degenerate binary recurrence sequence. Schinzel [11] in 1967 and Mignotte [8] in 1975 obtained estimates from below for u_n. Their estimates are not sufficiently precise for our purpose here. We shall require the following estimate which is taken from [13].

Lemma 5. *Let* K *be a field of degree* 2 *over the rationals and let* a, b, α, β *be non-zero numbers in* K *with* α *and* β *the roots of a monic quadratic polynomial with integer coefficients. Assume* $|\alpha| \geqq |\beta|$. *If* α/β *is not a root of unity then*

$$|a\alpha^n + b\beta^n| > |\alpha|^{n - C_1 \log n},$$

for $n > C_2$, *where* C_1 *and* C_2 *are positive numbers which are effectively computable in terms of* a *and* b *only.*

Proof. In what follows $c_1, c_2, \ldots$ will denote positive numbers which are effectively computable in terms of a and b only. Put $u_n = a\alpha^n + b\beta^n$ for $n = 1, 2, \ldots$. We first show that u_n is non-zero for $n > c_1$. If α/β is a unit in $Q(\alpha)$ then, since α/β is not a root of unity, the maximum of $|\alpha/\beta|$ and $|\beta/\alpha|$ is at least $(1 + \sqrt{5})/2$ as can be readily verified. Thus if $u_n = 0$ so that $-b/a = (\alpha/\beta)^n$, then $n < c_1$. If α/β is not a unit, then for some prime ideal $\mathfrak{p}$ of the ring of algebraic integers of $Q(\alpha)$, we have $\operatorname{ord}_{\mathfrak{p}}(\alpha/\beta)$ different from 0 and we see that $-b/a = (\alpha/\beta)^n$ implies $n < c_2$.

We shall now assume that $n > c_1 + c_2$. We then have

$$|u_n| = |a||\alpha|^n|(-b/a)(\beta/\alpha)^n - 1|, \tag{7}$$

and it is clear that the lemma depends upon obtaining a good lower estimate for

$$S = |(-b/a)(\beta/\alpha)^n - 1|. \tag{8}$$

For any complex number z either $|e^z - 1| > \frac{1}{2}$ or there exists some integer k for which $|z-ik\pi| \leqq 2|e^z-1|$. On putting $z=\log(-b/a)+n\log(\beta/\alpha)$ where the logarithms are assumed to take their principal values we deduce that either S is $>\frac{1}{2}$ or

$$S \geqq \tfrac{1}{2}|\log(-b/a)+n\log(\beta/\alpha)-ik\pi|$$

for some integer $k \leqq 2(n+1)$. We conclude from Lemma 1, on setting $\alpha_1 = -b/a$, $\alpha_2=-1$, $\alpha_3=\beta/\alpha$, $B=2(n+1)$, and $B'=n$ that

$$S > A^{-c_3 \log n},$$

where A denotes the height of α/β. Now $A \leqq 2|\alpha|^2$ and since $|\alpha| \geqq \sqrt{2}$, we have

$$S > |\alpha|^{-c_4 \log n}. \tag{9}$$

Our result now follows from (7), (8) and (9).

LEMMA 6. *Let α be a real algebraic number larger than one from a field K of degree D over Q. Further let d, a and b be non-zero numbers from K and let δ be a positive real number. If*

$$dx^q = a\alpha^n + b, \tag{10}$$

with $|b| < \alpha^{n(1-\delta)}$ and with x, q and n integers larger than one, then q is less than C, a number which is effectively computable in terms of D, d, a, α, and δ only.

PROOF. Let $c_1, c_2, \ldots$ be positive numbers which are effectively computable in terms of D, d, a, α, and δ. We shall assume that n is larger than c_1, where c_1 is chosen sufficiently large to ensure the validity of the subsequent arguments. Note that if $n < c_1$ and (10) holds then $q < c_2$, as required, since x is an integer larger than one.

From (10) we have

$$|dx^q| = |a\alpha^n + b| \geqq |a|\alpha^n - |b|.$$

Since $|b| < \alpha^{n(1-\delta)}$, we have $x^q \geqq c_3\alpha^n$, hence

$$\log x \geqq c_4 \frac{n}{q}. \tag{11}$$

Further

$$\frac{dx^q}{a\alpha^n} = 1 + \frac{b}{a\alpha^n}, \tag{12}$$

so

$$1-(|a|\alpha^{\delta n})^{-1} \leqq |d/a|\alpha^{-n}x^q \leqq 1+(|a|\alpha^{\delta n})^{-1}.$$

Now for n sufficiently large $(|a|\alpha^{\delta n})^{-1} < \frac{1}{2}$. On taking logarithms and recalling that $|\log(1+x)| \leqq x$ and $|\log(1-x)| \leqq 2x$ for $0 \leqq x < \frac{1}{2}$, we find that

$$(13) \qquad |\log|d/a| - n\log\alpha + q\log x| < c_5\alpha^{-\delta n} .$$

Put $\Lambda = \log|d/a| - n\log\alpha + q\log x$ and employ Lemma 1 with $n=3$, $D=D$, $\alpha_1 = |d/a|$, $\alpha_2 = \alpha$, $\alpha_3 = x$, $B' = q$, and $B = n$. From (12) and the fact that $b \neq 0$, we see that $\Lambda \neq 0$. Thus, by Lemma 1,

$$|\Lambda| > \exp\left(-c_6\left(\log q \log x + \frac{n}{q}\right)\right),$$

hence, by (11),

$$|\Lambda| > \exp(-c_7 \log q \log x) .$$

A comparison with (13) reveals that

$$(14) \qquad -\log q \log x < c_8 - c_9 n .$$

However,

$$x^q = (a\alpha^n + b)d^{-1} \leqq c_{10}\alpha^n .$$

Thus, for n sufficiently large, $c_{11}q\log x < n$ and from (14) we see that

$$c_{12}q\log x < c_{13} + \log q \log x .$$

Since x is at least two we conclude that

$$q < c_{14} ,$$

as required.

LEMMA 7. *Let d be a non-zero integer and let u_n be the n-th term of a non-degenerate binary recurrence sequence, as in* (2), *with α and β not real numbers. If*

$$dx^q = u_n ,$$

for an integer x larger than one and a prime q, then $q < C$, a number which is effectively computable in terms of a, α, b, β, and d only.

PROOF. Let $c_1, c_2, \ldots$ be positive numbers which are effectively computable in terms of a, α, b, β, and d only. We have

$$(15) \qquad dx^q = a\alpha^n + b\beta^n ,$$

with $ab \neq 0$ and α and β roots of a monic quadratic polynomial. Since α and β are not real they are complex conjugates and $|\alpha| = |\beta|$. We note that $|\alpha| = |\beta| > 1$, since otherwise α and β are roots of unity contrary to the assumption that u_n is non-degenerate. It is easy to verify that $|\alpha|=|\beta|\geqq\sqrt{2}$.

We have $x^q\leqq c_1|\alpha|^n$, hence

$$q\log x \leqq c_2 n\,. \tag{16}$$

By Lemma 5,

$$|dx^q| > |\alpha|^{n/2}\,,$$

for $n>c_3$, whence

$$\frac{n}{q} < c_4\log x\,. \tag{17}$$

since $|\alpha|\geqq\sqrt{2}$. Note that we may assume $n>c_3$ since otherwise the result follows from (16) and the fact that $x\geqq 2$.

Observe that α/β and β/α are conjugate algebraic numbers of degree 2 and, since $|\alpha|=|\beta|$, of absolute value one. Since α/β is not a root of unity and $Q(\alpha)$ has no units which are not roots of unity neither α/β nor β/α are algebraic integers. Thus there is a prime ideal $\mathfrak{p}$ in the ring of algebraic integers of $Q(\alpha)$ for which either $\operatorname{ord}_{\mathfrak{p}}\alpha/\beta$ or $\operatorname{ord}_{\mathfrak{p}}\beta/\alpha$ is positive. Assume without loss of generality that $\operatorname{ord}_{\mathfrak{p}}\alpha/\beta$ is positive. From (15) we find

$$\operatorname{ord}_{\mathfrak{p}}(db^{-1}x^q\beta^{-n}-1) = \operatorname{ord}_{\mathfrak{p}}(a/b)+n\operatorname{ord}_{\mathfrak{p}}(\alpha/\beta)\,. \tag{18}$$

The prime ideal $\mathfrak{p}$ lies above a rational prime p with $p<c_5$. We may assume that $q>c_6$, since otherwise the lemma holds. We now apply Lemma 2 to the expression on the left hand side of equality (18). We take $\alpha_1=db^{-1}$, $\alpha_2=\beta$, and $\alpha_3=x$ with $b_1=1$, $b_2=n$, and $b_3=q$. Note that q is not divisible by p, since q is a prime larger than p. By Lemma 2 and (18)

$$n\operatorname{ord}_{\mathfrak{p}}(\alpha/\beta) < c_6\left(\log q\log x+\frac{n}{q}\right)+c_7\,.$$

Therefore, from (17),

$$n < c_8\log q\log x\,,$$

and by (16)

$$q\log x < c_9\log q\log x\,,$$

hence $q<c_{10}$ as required.

3. Proof of Theorem 2.

We first remark that it suffices to assume that q is a prime since the theorem asserts that both x and q are bounded. By Lemma 6 and Lemma 7 we may assume $q<c_1$; here $c_1, c_2, \ldots$ are positive numbers which are effectively computable in terms of d, a, α, b, and β. Let $[x]$ denote the ideal generated by x in the ring of algebraic integers of $Q(\alpha)$. We have $([\alpha^2],[\beta^2])=[k]$, where k is a positive rational integer. Thus, for $n\geqq 1$,

$$u_{2n} = k^n\left(a\left(\frac{\alpha^2}{k}\right)^n+b\left(\frac{\beta^2}{k}\right)^n\right) \quad \text{and}$$

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

Now if u_{2n} or u_{2n+1} is equal to dx^q, then k^n divides dx^q, and we have $dx^qk^{-n}=d_1x_1^q$, where d_1 and x_1 are integers with $|d_1|\leqq|d|k^q$ and $0<x_1\leqq x$. Therefore it suffices to prove the theorem under the assumption that $[\alpha]$ and $[\beta]$ are coprime, for then we may apply the result to $d_1x_1^q=k^{-n}u_{2n+\delta}$ for $\delta=0$ or 1 to conclude that $n<c_2$ except in the case $x_1=1$. If $x_1=1$, however, we may appeal to Lemma 5 to conclude, since α/β is not a root of unity, that $n<c_3$. Thus $n<c_2+c_3$ and it follows directly that x and q are less than c_4 as required. Accordingly, we consider

$$dx^q = a\alpha^n+b\beta^n, \tag{19}$$

with $[\alpha]$ and $[\beta]$ coprime. Further since $[\alpha]$ and $[\beta]$ are coprime, we may assume, after a minor adjustment to the factors of x and d, that $[x]$ and $[\alpha]$ are coprime; in particular, it suffices to replace d by dk^q and x by x/k, where k is the greatest common divisor of x and the numerator of the norm of b. Let r be an integer such that ra and rb are algebraic integers. We may certainly choose $r<c_5$. If $q\geqq 3$, put $n=2m+\delta$ with $\delta=0$ or 1 so that, from (19),

$$rdx^q-ra\alpha^\delta(\alpha^m)^2 = rb\beta^n, \tag{20}$$

while if $q=2$ put $n=3m+\delta$ with $\delta=0$, 1, or 2 so that

$$rdx^2-ra\alpha^\delta(\alpha^m)^3 = rb\beta^n. \tag{21}$$

Since the greatest prime factor of Norm $(rb\beta^n)$ is less than c_6, we may apply Lemma 3 to (20) and (21) to conclude that $|x|<c_7$. Thus $|a\alpha^n+b\beta^n|<c_8$ and from Lemma 5 we see that $n\leqq c_9$. Our result now follows.

4. Proof of Theorem 1.

We have $ax^{2t}+bx^ty+cy^2=d$, so that

$$a(x^t-\alpha_1y)(x^t-\alpha_2y) = d, \tag{22}$$

where α_1 and α_2 are algebraic numbers of degree at most 2 over the rationals. We observe that if α_1 and α_2 are distinct rational numbers, or if α_1 and α_2 are not real, our result follows readily on inspection of (22). Since the condition $b^2-4ac\neq 0$ excludes the possibility that $\alpha_1=\alpha_2$, we may assume that α_1 and α_2 are real irrational numbers.

Let ε be the fundamental unit in $Q(\alpha_1)$. Choose π_1 with $1\leqq|\pi_1|\leqq\varepsilon$ so that $x^t-\alpha_1y=\pi_1\varepsilon^n$ for some integer n. Applying σ, the non-trivial element of the Galois group of $Q(\alpha_1)$ over Q, to both sides of the previous equality and recalling that ε is a unit we see that $x^t-\alpha_2y=\pm\sigma(\pi_1)\varepsilon^{-n}$. Put $\pm\sigma(\pi_1)=\pi_2$. Since $1\leqq|\pi_1|\leqq\varepsilon$ and $\pi_1\pi_2=da^{-1}$, the heights of π_1 and π_2 are less than c_1, where $c_1,c_2,\ldots$ are positive numbers which are effectively computable in terms of a, b, c, and d. Then

$$(23)\qquad (\alpha_2-\alpha_1)x^t = \alpha_2\pi_1\varepsilon^n-\alpha_1\pi_2\varepsilon^{-n}\,.$$

We may assume without loss of generality that $n\geqq 0$. Since ε is a real algebraic number larger than one, in fact at least $(1+\sqrt{5})/2$, we may apply Lemma 6 with $\delta=\frac{1}{2}$, $d=(\alpha_2-\alpha_1)$, $a=\alpha_2\pi_1$, $\alpha=\varepsilon$, and $b=-\alpha_1\pi_2\varepsilon^{-n}$. Certainly for $n>c_2$, we have $|b|<\varepsilon^{n/2}$ and hence, by Lemma 6, $t<c_3$. Note that if $n\leqq c_2$, then since x is an integer larger than one, we have $t<c_4$. Thus in either case $t<c_5$.

If in (23), $t\geqq 3$ we write $\alpha_2\pi_1\varepsilon^n$ in the form $\alpha_2\pi_1\varepsilon^\delta(\varepsilon^m)^2$ with δ either 0 or 1, while if $t=2$, we write $\alpha_2\pi_2\varepsilon^n$ as $\alpha_2\pi_1\varepsilon^{\delta'}(\varepsilon^{m_1})^3$ with δ' one of 0, 1, and 2. Since $[x]$ and $[\varepsilon]$ are coprime ideals, we may apply Lemma 3 to conclude that $|x|<c_6$. Since $t<c_5$, we also have that $|y|<c_7$ as required.

5. Proof of Theorem 3.

Let $c_1,c_2,\ldots$ be positive numbers which are effectively computable in terms of $d,a,\alpha_1,\ldots,\alpha_t$ and the coefficients and degrees of $P_2,\ldots,P_t$. We have

$$u_n = a_1\alpha_1^n+P_2(n)\alpha_2^n+\ldots+P_t(n)\alpha_t^n\,,$$

with $a_1\neq 0$ and $|\alpha_1|>|\alpha_j|$ for $j=2,\ldots,t$. We may assume that α_1 is positive by, if necessary, changing the sign of a_1. Further, since α is an algebraic integer with absolute value strictly larger than all its conjugates on taking the norm we see that either $\alpha_1>1$ or α_1 is one of 0 and 1. But if $\alpha_1=0$ or 1, then $u_n-a_1\alpha^n$ is zero and so we may assume $\alpha_1>1$. Put

$$b = P_2(n)\alpha_2^n+\ldots+P_t(n)\alpha_t^n, \quad\text{and}\quad d_1 = \max\{\text{degree}\,(P_i)\mid i=2,\ldots,t\}\,.$$

We may assume without loss of generality that $|\alpha_2|\geqq|\alpha_j|$ for $j=2,\ldots,t$. Then $|b|\leqq c_1n^{d_1}|\alpha_2|^n$. Put $\delta=(1-\theta)/2$, where $\theta=0$ if $|\alpha_2|\leqq 1$ and

$$\theta = \frac{\log|\alpha_2|}{\log\alpha_1}$$

otherwise. Since $\alpha_1>1$ we have

$$|b| < \alpha_1^{n(1-\delta)},$$

for $n>c_2$. By assumption $b=u_n-a_1\alpha^n$ is non-zero hence by Lemma 6 if $n>c_2$ and

$$dx^q = u_n, \tag{24}$$

then $q<c_3$. Certainly if $n\leqq c_2$ and (24) holds, then $q<c_4$, since x is an integer larger than one. Thus q is less than c_5 as required.

6. Proof of Theorem 4.

Let $c_2, c_3, \ldots$ denote positive numbers which are effectively computable in terms of a, b, c, d, a_1, b_1, c_1, and d_1. From (5), $a_1x^2+b_1xy+c_1y^2=d_1$, so that $a_1(x-\alpha_1y)(x-\alpha_2y)=d_1$. Note that if α_1 and α_2 are distinct and are not real quadratic irrationals, then x and y are bounded and the theorem follows directly. By assumption $b_1^2\neq 4a_1c_1$, so α_1 and α_2 are distinct, and therefore we may assume that α_1 and α_2 are real quadratic irrationals. Let ε be the fundamental unit in $Q(\alpha_1)$. Then $x-\alpha_1y=\pi_1\varepsilon^n$ with $1\leqq|\pi_1|\leqq\varepsilon$, for some integer n, and $x-\alpha_2y=\pi_2\varepsilon^{-n}$; as in the proof of Theorem 1 we see that the heights of π_1 and π_2 are less than c_2. We have

$$(\alpha_2-\alpha_1)y = \pi_1\varepsilon^n-\pi_2\varepsilon^{-n} \quad \text{and} \quad (\alpha_2-\alpha_1)x = \alpha_2\pi_1\varepsilon^n-\alpha_1\pi_2\varepsilon^{-n}.$$

Put $\gamma_1=\pi_1(\alpha_2-\alpha_1)^{-1}$ and $\gamma_2=\pi_2(\alpha_2-\alpha_1)^{-1}$. Then

$$x = \alpha_2\gamma_1\varepsilon^n-\alpha_1\gamma_2\varepsilon^{-n}, \quad \text{and} \tag{25}$$

$$y = \gamma_1\varepsilon^n-\gamma_2\varepsilon^{-n}. \tag{26}$$

We may assume without loss of generality that $n\geqq 0$. Further, we remark that it suffices to prove that $n<c_3$, since then, from (25) and (26), $|x|$ and $|y|$ are less than c_4 and so, from (6), $|z|$ and q are less than c_5. From (6), (25) and (26) we have

$$dz^q = (a\alpha_2^2+b\alpha_2+c)\gamma_1^2\varepsilon^{2n}-(2a\alpha_2\alpha_1+b(\alpha_2+\alpha_1)+2c)\gamma_1\gamma_2 + (a\alpha_1^2+b\alpha_1+c)\gamma_2^2\varepsilon^{-2n}. \tag{27}$$

Put

$$r = (a\alpha_2^2+b\alpha_2+c)\gamma_1^2 \quad \text{and}$$
$$s = -(2a\alpha_2\alpha_1+b(\alpha_2+\alpha_1)+2c)\gamma_1\gamma_2+(a\alpha_1^2+b\alpha_1+c)\gamma_2^2\varepsilon^{-2n}.$$

Note that $r\neq 0$, since by assumption α_2 is not a root of ax^2+bx+c and $a_1^{-1}d_1\neq 0$, hence $\gamma_1\neq 0$. Further, $s\neq 0$ for $n>c_6$, since $\varepsilon\geqq(1+\sqrt{5})/2$, $a_1^{-1}d_1\neq 0$, and α_1

is not a root of ax^2+bx+c. Thus we may assume that r and s are non-zero and we may apply Lemma 6 with $\delta=\frac{1}{2}$, $\alpha=\varepsilon$, $a=r$, and $b=s$ to (27) to conclude that $q<c_7$.

From (27) we obtain

$$d\varepsilon^{2n}z^q = (a\alpha_2^2+b\alpha_2+c)\gamma_1^2\varepsilon^{4n}-(2a\alpha_2\alpha_1+b(\alpha_2+\alpha_1)+2c)\gamma_1\gamma_2\varepsilon^{2n} + (a\alpha_1^2+b\alpha_1+c)\gamma_2^2 \,. \tag{28}$$

Observe that a solution of (28) in integers z and n yields a solution of the related equation

$$Dt^q = AX^4+BX^2+C\,,$$

in algebraic integers t and X from $Q(\alpha_1)$; here $D=d\varepsilon^m$, where $0\leqq m<q$ and $2n\equiv m \pmod q$,

$$\begin{aligned} A &= (a\alpha_2^2+b\alpha_2+c)\gamma_1^2\,, \\ B &= -(2a\alpha_2\alpha_1+b(\alpha_2+\alpha_1)+2c)\gamma_1\gamma_2\,, \\ C &= (a\alpha_1^2+b\alpha_1+c)\gamma_2^2 \end{aligned}$$

and the solution is given by $t=\varepsilon^{[2n/q]}z$ and $X=\varepsilon^n$. We observe that the polynomial AX^4+BX^2+C has 4 distinct roots, if $A\neq0$, $C\neq0$, and $B^2-4AC\neq0$. By assumption, α_1 and α_2 are not roots of ax^2+bx+c and $a_1^{-1}d_1\neq0$, hence also $\gamma_1\gamma_2$, is non-zero. Thus $A\neq0$ and $C\neq0$. Further, since $\gamma_1\gamma_2\neq0$, the condition $B^2-4AC\neq0$ is equivalent to $4ac(\alpha_2-\alpha_1)^2\neq b^2(\alpha_2-\alpha_1)^2$. But $b^2\neq4ac$ and, since $b_1^2\neq4a_1c_1$, $\alpha_1\neq\alpha_2$. Thus we may assume that AX^4+BX^2+C has four distinct roots. We now employ Lemma 4 to obtain $\|X\|<c_8$ and $\|t\|<c_9$ for each q with $2\leqq q<c_7$. But $\|X\|<c_8$ implies $n<c_{10}$ as required.

NOTE. A. Petho has informed us that he has proved independently a result similar in character to Theorem 2 of the present paper. He has proved with the hypotheses of Theorem 2 and subject to the additional assumption that r_1 and r_2 are coprime, where $u_n=r_1u_{n-1}+r_2u_{n-2}$, that x, q, and n are less than C, a number which is effectively computable in terms of a, α, b, β, and the greatest prime factor of d. Petho's result will appear in the Journal of Number Theory under the title "*Perfect powers in second order linear recurrences*".

REFERENCES

1. A. Baker, *A sharpening of the bounds for linear forms in logarithms* II, Acta Arith. 24 (1973), 33–36.
2. A. Baker, *Bounds for the solutions of the hyperelliptic equation*, Proc. Cambridge Philos. Soc. 65 (1969), 439–444.
3. A. Baker, *Transcendental number theory*, Cambridge University Press, Cambridge, 1975.

4. J. H. E. Cohn, *On square Fibonacci numbers*, J. London Math. Soc. 39 (1964), 537–540.
5. J. H. E. Cohn, *Lucas and Fibonacci numbers and some Diophantine equations*, Proc. Glasgow Math. Assoc. 7 (1965), 24–28.
6. J. H. E. Cohn, *Eight Diophantine equations*, Proc. London Math. Soc. 16 (1966), 153–166. Addendum, ibid., 17 (1967), 381.
7. S. V. Kotov, *Über die maximale Norm der Idealteiler des Polynoms $\alpha x^m + \beta y^n$ mit den algebraischen Koeffizienten*, Acta Arith. 31 (1976), 219–230.
8. M. Mignotte, *A note on linear recursive sequences*, J. Austral. Math. Soc. Ser. A 20 (1975), 242–244.
9. L. J. Mordell, *Diophantine equations* (Pure and Applied Mathematics 30), Academic Press, London, New York, 1969.
10. A. J. van der Poorten, *Linear forms in logarithms in the p-adic case* in *Transcendence theory: advances and applications* (Proc. Conf., University of Cambridge, Cambridge 1976), eds. A. Baker and D. W. Masser, pp. 29–57, Academic Press, London, New York, 1977.
11. A. Schinzel, *On two theorems of Gelfond and their applications*, Acta Arith. 13 (1967), 177–236.
12. T. N. Shorey and R. Tijdeman, *New applications of Diophantine approximations to Diophantine equations*, Math. Scand. 39 (1976), 5–18.
13. C. L. Stewart, *Divisor properties of arithmetical sequences*, Ph. D. Thesis, University of Cambridge, 1976.
14. O. Wyler, *Squares in the Fibonacci series*, Amer. Math. Monthly 71 (1964), 220–222.

T. N. SHOREY
SCHOOL OF MATHEMATICS
TATA INSTITUTE OF FUNDAMENTAL RESEARCH
HOMI BHABHA ROAD
BOMBAY 400 005
INDIA

AND

C. L. STEWART
DEPARTMENT OF PURE MATHEMATICS
UNIVERSITY OF WATERLOO
WATERLOO, ONTARIO
CANADA, N2L 3G1