ACTA ARITHMETICA
LIV (1989)

Bounding squares in second order recurrence sequences

by

J. WOLFSKILL (DeKalb, Ill.)

1. Consider a second order linear recurrence sequence $x_n = \mathrm{Tr}(\alpha\theta^n)$, where θ is an algebraic integer in a real quadratic field $\boldsymbol{Q}(\sqrt{d})$ and $\alpha \in \boldsymbol{Q}(\sqrt{d})$; we assume here that the roots of the characteristic polynomial are real and irrational. The main result of this paper, roughly stated, is that if a large enough square occurs in this sequence, then one may bound explicitly further occurrences of squares, not only in the original sequence, but also in related sequences $\mathrm{Tr}(\beta\theta^n)$, where $\alpha\beta$ is a square in $\boldsymbol{Q}(\sqrt{d})$. This result, however, applies only to terms in the sequences whose exponents have the same parity as that for the term which is a large square. In some cases, for example when α is a square in $\boldsymbol{Q}(\sqrt{d})$, this "parity problem" can be disposed of on elementary grounds; but in general it poses a restriction on the applicability of the method. A more severe restriction is that the known square must be large enough; we quantify this statement in Section 2. Although a randomly selected sequence probably will not have a large enough square in it, many favorable examples exist; we list some in Section 3. In fact, infinitely many examples exist, and it is possible to construct them at will.

Some work has been done in the past on classifying the squares in specific sequences, beginning with Cohn's classification [3] of the squares in the Fibonacci and Lucas sequences. Tzanakis [11] adapted and extended Cohn's method in the course of solving several diophantine equations. His results may be viewed as classifying the squares in certain recurrence sequences. Apparently, it is not possible to prove a general result by this method, however.

General results on this problem have been obtained by Pethö [7] and Shorey and Stewart [8], [9] using Baker's method. An account of these and related results may be found in Chapter 9 of the recent book of Shorey and Tijdeman [10]. These results have the virtue of great generality, bounding not only occurrences of squares, but also higher powers, or even a fixed constant times a power. However, these results are difficult to apply, because the sizes of the constants are not indicated (presumably, they are quite large), nor is the manner in which the constants depend on the parameters involved.

We focus our attention mainly on sequences $x_n = \mathrm{Tr}(\alpha\varepsilon^n)$ with ε a unit (which may as well be assumed to be fundamental). There are two reasons for this: first, our results are better in this case; and second, we were led to this problem by considering diophantine equations of the form $y^2 - dx^4 = m$, in which x^2 naturally can be represented as a member of one or more such sequences. As this type of equation represents an elliptic curve, Baker and Coates [1] have given explicit, but large, upper bounds on the solutions. In some cases, their bounds have been applied successfully to the practical solution of a specific equation, as in the work of Ellison *et al.* [4] on $y^2 + 28 = x^3$. Ljunggren [6] has shown that the equation $Ax^2 - By^4 = C$, with A and B positive and $C = 1$, 2, or 4, has at most two solutions, and these (if they exist) can be found once the fundamental units in a certain quartic field are known. Ljunggren's results are equivalent to classifying, or giving an algorithm to classify, the squares in certain special reccurrence sequences. The method of Baker and Coates more generally gives an algorithm, at least in principle, to classify the squares in sequences $x_n = \mathrm{Tr}(\alpha\varepsilon^n)$. However, the general practical value of such an algorithm is not clear.

The method used in this paper is motivated by the analogy between the present problem,

$$x^2 = \alpha\varepsilon^n + \bar{\alpha}\bar{\varepsilon}^n \tag{1}$$

(bar denotes conjugation), and the generalized Ramanujan–Nagell equation

$$x^2 = 2^n + D \tag{2}$$

treated so successfully by Beukers in [2]. We adapt his method, based on hypergeometric polynomials, to prove a diophantine approximation result (Theorem 1) of the following form: if in (1) x is large enough, then one has a good lower bound

$$\left|\frac{y}{\sqrt{\alpha}\varepsilon^{m/2}} - 1\right| > \frac{C}{\varepsilon^{mv}} \tag{3}$$

for all integers y and m, with $m > n$ of the same parity. Here C is a constant depending on the "initial approximation" in (1) but not on m. The crucial thing is the exponent v, which is detemined by how large the inital square is. To be successful, one must have $v < 2$, since (see Lemma 5) if $y^2 = \mathrm{Tr}(\alpha\varepsilon^m)$ and y is large, then

$$\left|\frac{y}{\sqrt{\alpha}\varepsilon^{m/2}} - 1\right| \approx \frac{|\bar{\alpha}|}{2\alpha\varepsilon^{2m}}. \tag{4}$$

Comparison of (3) and (4) immediately leads to an upper bound on m, assuming $v < 2$. More generally, instead of (3) one may work with $\left|\frac{y}{\sqrt{\beta}\varepsilon^{m/2}} - 1\right|$, provided that $\alpha\beta$ is a square in $Q(\sqrt{d})$; the exponent v depends on the initial square in (1) only, and not on β.

Whether or not a large square exists in the sequence, (3) leads to a good bound on the number of squares. This follows from a separation result (Lemma 6) on consecutive squares, which states roughly that $m > 2k$ if x_k and x_m are both squares, with $m > k$ of the same parity. We show that if $|\bar{\alpha}| \leqslant \alpha$, there are at most 14 "large" squares; otherwise, the number of large squares is $O(\log\log(|\bar{\alpha}|/\alpha))$. In either case there are $O(\log H(\alpha)/\log\varepsilon)$ "small" squares. (By $H(\alpha)$ we mean the height of α, that is, the largest coefficient in its minimal polynomial.) We refer the reader to Theorem 2 for a precise statement of how large "large" is.

As the referee kindly pointed out to me, it is posssible to view an occurrence of a square in the sequence $x_n = \mathrm{Tr}(\alpha\varepsilon^n)$ as a solution to a certain equation in S-units; then applying Theorem 1 of [5] leads to an upper bound on the number of squares. We have

$$\lambda X + \mu Y = 1,$$

where

$$\lambda = \frac{1}{2\sqrt{\alpha}}, \quad \mu = \frac{-1}{2\sqrt{\alpha}}, \quad X = \frac{x}{\varepsilon^{n/2}} + \sqrt{\alpha}, \quad \text{and} \quad Y = \frac{x}{\varepsilon^{n/2}} - \sqrt{\alpha}.$$

If $x_n = x^2$, then $XY = \pm\bar{\alpha}\bar{\varepsilon}^{2n}$, so any prime dividing X or Y must divide $\bar{\alpha}$. In the worst case, the field $K = Q(\sqrt{\varepsilon}, \sqrt{\alpha})$ is totally real of degree 8, and Theorem 1 of [5] gives a bound of $3\cdot 7^{24+2t}$ solutions X and Y, where t is the number of primes dividing $\bar{\alpha}$ in K. As the bound to be derived here depends instead on the height of α, the two results are not directly comparable. For α of very large height, with a small number of prime divisors, Evertse's theorem yields a better bound.

It should be emphasized that throughout the paper we work with x_n for $n \geqslant 0$ only. A diophantine equation of the form $y^2 - dx^4 = m$ leads naturally to $\pm x^2$ being in one or more recurrence sequences $x_n = \mathrm{Tr}(\alpha\varepsilon^n)$, for various values of α. Thus one is interested in the more general problem $x_{\pm n} = \pm x^2$. However, the cases of one or both minus signs can always be reformulated as $x_n = x^2$ for $n \geqslant 0$, by replacing α by $\pm\bar{\alpha}$. Thus the restriction $n \geqslant 0$ imposes no essential loss of generality.

I wish to thank my colleague Tom Cusick for several valuable discussions about this work. In addition, I am deeply grateful for the referee's comments; in particular, the separation lemma is due to the referee.

2. Let n_1 and n_2 be positive integers, $n_2 \geqslant n_1$, and let $n = n_1 + n_2$. We define polynomials G and H by

$$G(z) = \sum_{j=0}^{n_1} \frac{\binom{n_2+\frac{1}{2}}{j}\binom{n_1}{j}}{\binom{n}{j}}(-z)^j, \quad H(z) = \sum_{j=0}^{n_2} \frac{\binom{n_1-\frac{1}{2}}{j}\binom{n_2}{j}}{\binom{n}{j}}(-z)^j. \tag{5}$$

These are hypergeometric polynomials: $G(z) = F(-n_2-\frac{1}{2}, -n_1, -n, z)$ and $H(z) = F(-n_1+\frac{1}{2}, -n_2, -n, z)$, where F is the usual hypergeometric function. What is relevant for our purposes is that $G(z)/H(z)$ approximates $\sqrt{1-z}$ very well for small z (see below). From Lemmas 2, 3, and 4 of [2] we summarize the following information about G and H:

LEMMA 1. 1. $\binom{n}{n_1}G(4z)$ *and* $\binom{n}{n_1}H(4z)$ *have integral coefficients.*

2. $|G(z)-\sqrt{1-z}H(z)| < G(1)|z|^{n+1}$ *for* $|z| < 1$.

3. $\binom{n}{n_1}G(1) = \prod_{j=1}^{n_1}\left(1-\frac{1}{2j}\right)$.

4. *Let* G^* *and* H^* *be defined as in* (5) *with* n_1 *and* n_2 *replaced by* n_1+1 *and* n_2+1. *Then*

$$G^*(z)H(z)-G(z)H^*(z) = cz^{n+1}, \quad \text{with } c \neq 0.$$

It is necessary to establish a few other simple lemmas before proving the main theorem. Throughout this paper, G and H are defined as in (5).

LEMMA 2. *For all* z,

$$|G(z)| < (1+|z|)^{n_1} \quad \text{and} \quad |H(z)| < (1+|z|)^{n_2}.$$

Proof. This follows directly from (5), since $n > n_2+\frac{1}{2}$ and $n > n_1-\frac{1}{2}$. So

$$|G(z)| < \sum_{j=0}^{n_1}\binom{n_1}{j}|z|^j = (1+|z|)^{n_1},$$

and similarly for H.

LEMMA 3.

$$\binom{n}{n_1}G(1) < \frac{1}{\sqrt{n_1}}.$$

Proof. It is simple to prove by induction that the product in (3) of Lemma 1 is at most $(2\sqrt{n_1}-1)/2n_1$, which is a stronger inequality than the lemma asserts.

LEMMA 4. *Let* n *and* k *be positive integers such that* $n \geq 4k-3$. *Then*

$$\binom{n}{k} < \left(\frac{4}{3^{3/4}}\right)^n.$$

Proof. Since

$$\binom{4m+4}{m+1} = \frac{(4m+4)(4m+3)(4m+2)(4m+1)}{(m+1)(3m+3)(3m+2)(3m+1)}\binom{4m}{m} < \frac{4^4}{3^3}\binom{4m}{m},$$

it follows by induction that

$$\binom{4m}{m} < \left(\frac{4^4}{3^3}\right)^{m-1}\binom{4}{1} = \left(\frac{4}{3^{3/4}}\right)^{4m}\frac{27}{64}.$$

Hence also

$$\binom{4m-1}{m} = \binom{4m}{m}\frac{3}{4} < \left(\frac{4}{3^{3/4}}\right)^{4m-1}\frac{3^{13/4}}{64}.$$

Similarly,

$$\binom{4m-2}{m} < \left(\frac{4}{3^{3/4}}\right)^{4m-2}\frac{3^{14/4}}{64},$$

and

$$\binom{4m-3}{m} < \left(\frac{4}{3^{3/4}}\right)^{4m-3}\frac{3^{15/4}}{64}.$$

Since $n \geq 4k-3$, $\binom{n}{k} \leqslant \binom{n}{m}$, where $m = \left[\frac{n+3}{4}\right]$, and this has one of the four forms treated above. Hence

$$\binom{n}{k} < \left(\frac{4}{3^{3/4}}\right)^n\frac{3^{15/4}}{64} < \left(\frac{4}{3^{3/4}}\right)^n.$$

In order to simplify the statement of Theorem 1, it is expedient to define beforehand some of the parameters involved. Throughout this section, we use the following notation:

$Q(\sqrt{d})$ is a real quadratic field.

Bar denotes conjugation in $Q(\sqrt{d})$.

$\varepsilon > 1$ is a unit in $Q(\sqrt{d})$.

$x_n = \mathrm{Tr}(\alpha\varepsilon^n)$ is a given recurrence sequence with $\alpha > 0$ in $Q(\sqrt{d})$.

$\bar{\alpha}/\alpha = \pm\bar{\zeta}/\zeta$ with $\zeta > 0$ an algebraic integer.

$\beta \in Q(\sqrt{d})$ such that $\alpha\beta$ is a square in $Q(\sqrt{d})$.

$\sqrt{\beta/\alpha} = \gamma/a$ where a is a positive integer, and γ is an algebraic integer.

$\eta = \max(\gamma, |\bar{\gamma}|)$, $\varphi = \max\left(\frac{\zeta}{|\bar{\zeta}|}, \frac{|\bar{\zeta}|}{\zeta}\right)$, and $N = |\zeta\bar{\zeta}|$.

THEOREM 1. *For some* $k \geq 1$, *let* $x_k = x^2$, *a perfect square in* $\mathbf{Z}$. *Let* $z_0 = -\bar{\alpha}\bar{\varepsilon}^k/\alpha\varepsilon^k$, *and assume* $\sigma < 1/2$, *where*

$$\sigma = \frac{3\log 4 - \frac{3}{4}\log 3 + \log(1+|z_0|) + \log N}{2k\log\varepsilon + \frac{3}{2}\log 3 - 4\log 4 - \log(1+|z_0|) - 2\log|\bar{\zeta}|}. \tag{6}$$

Let $y > 0$ *and* m *be integers; assume that* $m \geq k$ *with the same parity, and*

$$m \geq \left(2k + \frac{\log(\zeta/|\bar{\zeta}|)}{\log\varepsilon}\right)\left(\frac{1}{2} + \frac{1}{\sigma}\cdot\frac{\alpha^2\gamma^2\eta^2\varphi}{2^{10}\zeta^2N^2}\right). \tag{7}$$

Define v *by*

$$v = 1 + 2\sigma + \frac{(1+2\sigma)\log 4 - (\frac{3}{4}+\frac{3}{2}\sigma)\log 3 + \sigma\log(1+|z_0|)}{2k\log\varepsilon + \log(\zeta/|\bar{\zeta}|)}. \tag{8}$$

Then

$$\left|\frac{y}{\sqrt{\beta}\varepsilon^{m/2}}-1\right|>\frac{C}{\varepsilon^{m\nu}}, \tag{9}$$

where

$$C=\frac{3^5}{2^{25}\alpha\gamma\eta\varphi^{(\nu+1)/2}\zeta^4(1+|z_0|)^{9/2}\varepsilon^{k(5+\nu)}}.$$

Note. The reader may prefer first to consider the situation $\alpha=\beta=1$, in which case ζ, N, φ, a, γ, and η all disappear from (6), (8), and (9), and (7) may be discarded.

Proof. It follows from (6) and the condition $\sigma<1/2$ that

$$\frac{\varepsilon^{2k}3^{3/2}}{4^4(1+|z_0|)|\bar{\zeta}|^2}>\frac{4^6}{3^{3/2}}(1+|z_0|)^2N^2,$$

which implies that $\varepsilon^{2k}>4^{10}3^{-3}\,|\bar{\zeta}|^2$, and thus $|z_0|=|\bar{\zeta}|/\zeta\varepsilon^{2k}<3^3/4^{10}<1$. We will apply (2) of Lemma 1, with $z=z_0$ (n_1 and n_2 will be selected later, with $n_2\geqslant n_1$). Multiplying by $\binom{n}{n_1}$, where $n=n_1+n_2$, we have

$$\left|\binom{n}{n_1}G(z_0)-\sqrt{1-z_0}\binom{n}{n_1}H(z_0)\right|<\binom{n}{n_1}G(1)|z_0|^{n+1}. \tag{10}$$

Since $z_0=\pm\bar{\zeta}/\zeta\varepsilon^{2k}$, with denominator ζ,

$$\binom{n}{n_1}G(z_0)=\frac{A}{(4\zeta)^{n_1}}\quad\text{and}\quad\binom{n}{n_1}H(z_0)=\frac{B}{(4\zeta)^{n_2}}$$

for some algebraic integers A and B in $\boldsymbol{Q}(\sqrt{d})$, by (1) of Lemma 1. Further,

$$\sqrt{1-z_0}=x/\sqrt{\alpha}\varepsilon^{k/2}$$

so (10) becomes

$$\left|\frac{A}{(4\zeta)^{n_1}}-\frac{xB}{\sqrt{\alpha}\varepsilon^{k/2}(4\zeta)^{n_2}}\right|<\frac{\binom{n}{n_1}G(1)|\bar{\zeta}|}{\zeta\varepsilon^{2k}}\cdot\frac{|\bar{\zeta}|^n}{\zeta^n\varepsilon^{2kn}}.$$

Using Lemma 3 and rearranging, we have

$$\left|1-\frac{xB}{\sqrt{\alpha}\varepsilon^{k/2}A(4\zeta)^{\lambda}}\right|<\frac{|\bar{\zeta}|}{\sqrt{n_1}\zeta\varepsilon^{2k}}\cdot\frac{4^{n_1}|\bar{\zeta}|^n}{|A|\zeta^{n_2}\varepsilon^{2kn}},$$

where $\lambda=n_2-n_1$. We denote

$$\delta=\left|\frac{y}{\sqrt{\beta}\varepsilon^{m/2}}-1\right|$$

and add to the above to get

$$\left|\frac{y}{\sqrt{\beta}\varepsilon^{m/2}}-\frac{xB}{\sqrt{\alpha}\varepsilon^{k/2}A(4\zeta)^{\lambda}}\right|<\delta+\frac{|\bar{\zeta}|}{\sqrt{n_1}\zeta\varepsilon^{2k}}\cdot\frac{4^{n_1}|\bar{\zeta}|^n}{|A|\zeta^{n_2}\varepsilon^{2kn}}. \tag{11}$$

The left side of (11) is

$$\left|\frac{yaA(4\zeta)^{\lambda}-xB\gamma\varepsilon^{(m-k)/2}}{\gamma\sqrt{\alpha}\varepsilon^{m/2}A(4\zeta)^{\lambda}}\right|. \tag{12}$$

Let K be the numerator of the fraction in (12); K is an algebraic integer in $\boldsymbol{Q}(\sqrt{d})$. We can insure that $K\neq 0$ by the following standard device: n_1 will be selected in the range

$$\sigma\lambda\leqslant n_1<\sigma\lambda+2 \tag{13}$$

(λ is specified later, in terms of m). This allows 2 consecutive choices for n_1, and 2 corresponding consecutive choices for n_2, as λ is fixed. If K were zero for both choices, then in (4) of Lemma 1 G/H and G^*/H^* would have equal values at z_0, and this is impossible.

Since K is a nonzero algebraic integer, $|K|\geqslant|\bar{K}|^{-1}$. We have

$$|\bar{K}|\leqslant ya|\bar{A}|(4|\bar{\zeta}|)^{\lambda}+x|\bar{B}||\bar{\gamma}|\varepsilon^{(k-m)/2}.$$

Now,

$$|\bar{A}|=\left|\binom{n}{n_1}(4|\bar{\zeta}|)^{n_1}G(\bar{z}_0)\right|<\binom{n}{n_1}4^{n_1}|\bar{\zeta}|^{n_1}\left(1+\frac{\zeta\varepsilon^{2k}}{|\bar{\zeta}|}\right)^{n_1}$$
$$=\binom{n}{n_1}(4\zeta\varepsilon^{2k})^{n_1}(1+|z_0|)^{n_1},$$

by Lemma 2, and similarly,

$$|\bar{B}|<\binom{n}{n_1}(4\zeta\varepsilon^{2k})^{n_2}(1+|z_0|)^{n_2}.$$

There is no loss of generality in assuming $\delta<1$ (the constant C is less than one); hence $y<2\sqrt{\beta}\varepsilon^{m/2}$. Also,

$$x=\sqrt{\alpha\varepsilon^k+\bar{\alpha}\bar{\varepsilon}^k}\leqslant\sqrt{\alpha}\varepsilon^{k/2}\sqrt{1+|z_0|}.$$

Thus

$$\begin{aligned}|\bar{K}|&<2\sqrt{\beta}\varepsilon^{m/2}a\binom{n}{n_1}(4\zeta\varepsilon^{2k})^{n_1}(1+|z_0|)^{n_1}(4|\bar{\zeta}|)^{\lambda}\\&\quad+\sqrt{\alpha}\varepsilon^{k/2}\sqrt{1+|z_0|}\binom{n}{n_1}(4\zeta\varepsilon^{2k})^{n_2}(1+|z_0|)^{n_2}|\bar{\gamma}|\varepsilon^{(k-m)/2}\\&<\sqrt{\alpha}4^{n_2}\binom{n}{n_1}(1+|z_0|)^{n_2+1/2}\zeta^{n_1}(2\gamma\varepsilon^{m/2+2kn_1}|\bar{\zeta}|^{\lambda}+|\bar{\gamma}|\varepsilon^k\varepsilon^{2kn_2-m/2}\zeta^{\lambda}).\end{aligned} \tag{14}$$

At this point we are ready to specify λ; let λ be the nearest integer to

$$\frac{m}{2k+\dfrac{\log(\zeta/|\bar{\zeta}|)}{\log\varepsilon}},$$

and let the remainder be μ, with $-\frac{1}{2}<\mu\leqslant\frac{1}{2}$. Then

$$\varepsilon^m=\left(\varepsilon^{2k}\frac{\zeta}{|\bar{\zeta}|}\right)^{\lambda+\mu}. \tag{15}$$

Using (15) simplifies (14) to

$$|\bar{K}|<\sqrt{\alpha}4^{n_2}\binom{n}{n_1}(1+|z_0|)^{n_2+1/2}\zeta^{n_1}\varepsilon^{kn}N^{\lambda/2}\times\left(2\gamma\varepsilon^{k\mu}\left(\frac{\zeta}{|\bar{\zeta}|}\right)^{\mu/2}+|\bar{\gamma}|\varepsilon^{k(1-\mu)}\left(\frac{|\bar{\zeta}|}{\zeta}\right)^{\mu/2}\right).$$

The second term in parentheses has the higher power of ε, and we may condense this, via η and φ, to

$$|\bar{K}|<\sqrt{\alpha}4^{n_2}\binom{n}{n_1}(1+|z_0|)^{n_2+1/2}\zeta^{n_1}\varepsilon^{kn}N^{\lambda/2}3\eta\varphi^{1/4}\varepsilon^{k(1-\mu)}.$$

Combining this with (12) and (11), we have

$$\left[\sqrt{\alpha}\gamma\varepsilon^{m/2}|A|(4\zeta)^{\lambda}\sqrt{\alpha}4^{n_2}\binom{n}{n_1}(1+|z_0|)^{n_2+1/2}\zeta^{n_1}\varepsilon^{kn}N^{\lambda/2}3\eta\varphi^{1/4}\varepsilon^{k(1-\mu)}\right]^{-1}<\delta+\frac{|\bar{\zeta}|}{\sqrt{n_1}\zeta\varepsilon^{2k}}\cdot\frac{4^{n_1}|\bar{\zeta}|^n}{|A|\zeta^{n_2}\varepsilon^{2kn}}. \tag{16}$$

Let L be the denominator of the left side of (16), so

$$L=3\alpha\gamma\eta\varphi^{1/4}\varepsilon^{k(1-\mu)}|A|\binom{n}{n_1}4^{n_2+\lambda}\zeta^{n_2}(1+|z_0|)^{n_2+1/2}N^{\lambda/2}\varepsilon^{m/2+kn}. \tag{17}$$

Then (16) implies that

$$1<\delta L+\frac{|\bar{\zeta}|3\alpha\gamma\eta\varphi^{1/4}}{\sqrt{n_1}\zeta\varepsilon^{k(1+\mu)}}\cdot\frac{4^{2n_2}\binom{n}{n_1}(1+|z_0|)^{n_2+1/2}N^{\lambda/2}|\bar{\zeta}|^n\varepsilon^{m/2}}{\varepsilon^{kn}}. \tag{18}$$

By (15), and since $|\mu|\leqslant\frac{1}{2}$, the second term on the right is $\leqslant$

$$\frac{|\bar{\zeta}|3\alpha\gamma\eta\varphi^{1/2}\sqrt{1+|z_0|}}{\sqrt{n_1}\zeta\varepsilon^{k}}\cdot\frac{4^{2n_2}\binom{n}{n_1}(1+|z_0|)^{n_2}N^{\lambda}|\bar{\zeta}|^{2n_1}}{\varepsilon^{2kn_1}}. \tag{19}$$

We claim that the first factor is $<1/2$, and the second $\leqslant 1$. By (6), since $\sigma<\frac{1}{2}$, we have

$$\varepsilon^k>\frac{2^{10}(1+|z_0|)^{3/2}N|\bar{\zeta}|}{3^{3/2}},$$

so the first factor of (19) is less than

$$\frac{3^{5/2}\alpha\gamma\eta\varphi^{1/2}}{\sqrt{n_1}2^{10}\zeta N}<\frac{\alpha\gamma\eta\varphi^{1/2}}{\sqrt{n_1}2^{6}\zeta N}$$

as $3^5<2^8$. By (7), (13), and (15),

$$n_1\geqslant\sigma\lambda\geqslant\sigma.\left[\frac{m}{2k+\dfrac{\log(\zeta/|\bar{\zeta}|)}{\log\varepsilon}}-\frac{1}{2}\right]\geqslant\frac{\alpha^2\gamma^2\eta^2\varphi}{2^{10}\zeta^2N^2},$$

and this shows that the first factor of (19) is $<1/2$. From (13), $n_1<\frac{1}{2}\lambda+2$ and this shows that $n\geqslant 4n_1-3$. Hence, by Lemma 4, the second factor of (19) is smaller than

$$\frac{4^{2n_1+2\lambda}\left(\dfrac{4}{3^{3/4}}\right)^{2n_1+\lambda}(1+|z_0|)^{n_1+\lambda}N^{\lambda}|\bar{\zeta}|^{2n_1}}{\varepsilon^{2kn_1}}\leqslant\left[\frac{4^{2+2/\sigma}\left(\dfrac{4}{3^{3/4}}\right)^{2+1/\sigma}(1+|z_0|)^{1+1/\sigma}N^{1/\sigma}|\bar{\zeta}|^{2}}{\varepsilon^{2k}}\right]^{n_1}$$

by (13). The bracket equals 1 by (6). Thus, (18) becomes

$$1<\delta L+\frac{1}{2},\quad\text{i.e.,}\quad\delta>\frac{1}{2L}. \tag{20}$$

From (15) and (17),

$$2L=\left(6\alpha\gamma\eta\varphi^{1/4}\varepsilon^{k}\left(\frac{\zeta}{|\bar{\zeta}|}\right)^{\mu/2}\sqrt{1+|z_0|}\right)\left(|A|\binom{n}{n_1}4^{n_2+\lambda}\zeta^{n_2+\lambda}(1+|z_0|)^{n_2}\varepsilon^{2kn_2}\right). \tag{21}$$

The first factor of (21) is $\leqslant 6\alpha\gamma\eta\varphi^{1/2}\sqrt{1+|z_0|}\varepsilon^k$. To estimate the second factor,

$$|A|=\binom{n}{n_1}(4\zeta)^{n_1}|G(z_0)|<\binom{n}{n_1}(4\zeta)^{n_1}(1+|z_0|)^{n_1}$$

by Lemma 2. Hence, using Lemma 4, the second factor of (21) is less than

$$4^{2n_2}\left(\frac{4}{3^{3/4}}\right)^{2n}\zeta^{2n_2}(1+|z_0|)^n\varepsilon^{2kn_2}=\left(\varepsilon^{2k}\frac{\zeta}{|\bar{\zeta}|}\right)^{n_2}N^{n_2}4^{2n_2}\left(\frac{4}{3^{3/4}}\right)^{2n}(1+|z_0|)^n.$$

By (13), this is at most

$$\text{(22)}\quad \left[\left(\varepsilon^{2k}\frac{\zeta}{|\bar{\zeta}|}\right)^{1+\sigma}N^{1+\sigma}4^{2+2\sigma}\left(\frac{4}{3^{3/4}}\right)^{2+4\sigma}(1+|z_0|)^{1+2\sigma}\right]^{\lambda}\times\left[\varepsilon^{2k}\zeta^2 4^2\frac{4^4}{3^3}(1+|z_0|)^2\right]^2.$$

The first bracket is, by (8) and (15),

$$\left(\varepsilon^{2k}\frac{\zeta}{|\bar{\zeta}|}\right)^{\nu\lambda}=\varepsilon^{m\nu}\left(\varepsilon^{2k}\frac{\zeta}{|\bar{\zeta}|}\right)^{-\mu\nu}\leqslant\varepsilon^{m\nu}\varepsilon^{k\nu}\varphi^{\nu/2}.$$

Finally, combining (20), (21), and (22) achieves the lower bound (9), and the theorem is proved.

Several remarks are in order concerning this theorem:

1. It should be noted that σ and ν depend on α, ε, and k only, and not on β. Thus, one successful instance of the theorem leads to good lower bounds (9) for an entire family of recurrence sequences.

2. In applying the theorem, it is necessary that $\nu<2$; compare (9) with Lemma 5 in the next section.

3. The condition (7) is not really a loss of generality, in the sense that the ultimate goal is to bound m anyway.

4. If m and k have opposite parity, or if $\alpha\beta$ is not a square in $Q(\sqrt{d})$, then in (12) K becomes an element of a 4th degree field. The lower bound that $|K|$ is at least the product of the reciprocals of its conjugates is then so poor that the method fails altogether.

3. In this section we discuss briefly some examples illustrating Theorem 1. First we show explicitly that a successful instance (i.e. $\nu<2$) of Theorem 1 leads to an upper bound on m.

LEMMA 5. *Let $y_n=\mathrm{Tr}(\beta\varepsilon^n)$, where ε is a unit in $Q(\sqrt{d})$, and $\beta>0$ is in $Q(\sqrt{d})$. If $y_m=y^2$, with y a positive integer, then*

$$\text{(23)}\quad \left|\frac{y}{\sqrt{\beta}\varepsilon^{m/2}}-1\right|<\frac{|\bar{\beta}|}{\beta\varepsilon^{2m}}.$$

Proof. We have

$$y^2=\beta\varepsilon^m+\bar{\beta}\bar{\varepsilon}^m=\beta\varepsilon^m\left(1\pm\frac{\bar{\beta}}{\beta\varepsilon^{2m}}\right).$$

Hence

$$\left|\frac{y}{\sqrt{\beta}\varepsilon^{m/2}}-1\right|=\frac{|\bar{\beta}|}{\beta\varepsilon^{2m}}\left|\frac{y}{\sqrt{\beta}\varepsilon^{m/2}}+1\right|^{-1}<\frac{|\bar{\beta}|}{\beta\varepsilon^{2m}}.$$

If we are in a situation in which Theorem 1 applies, comparison of (9) and (23) shows that

$$\text{(24)}\quad m<k\cdot\frac{5+\nu}{2-\nu}+\frac{\log C_1}{(2-\nu)\log\varepsilon},$$

where

$$\text{(25)}\quad C_1=\frac{2^{25}\alpha|\bar{\beta}|\gamma\eta\zeta^4\varphi^{(\nu+1)/2}(1+|z_0|)^{9/2}}{3^5\beta}.$$

The following four sequences have a large enough square in them for Theorem 1 to apply:

1. $\{0, 1, 2, 5, \ldots\}$, with $x_{n+2}=2x_{n+1}+x_n$. Here $x_7=169$.
2. The Fibonacci sequence, where $x_{12}=144$.
3. $\{1, 3, 65, 1427, \ldots\}$, with $x_{n+2}=22x_{n+1}-x_n$. Here $x_4=31329=177^2$.
4. $\{2, 12, 146, 1764, \ldots\}$, with $x_{n+2}=12x_{n+1}+x_n$. Here $x_3=1764=42^2$.

In the following table, we list the values of σ, ν, and the upper bound on m in (24), for these four sequences (σ and ν have been rounded to four decimal places).

Seq.	σ	ν	$m\leqslant$
1	.3950	1.8717	469
2	.4358	1.9628	2862
3	.3661	1.7749	142
4	.3017	1.6637	73

In each case, the upper bound applies only for m with the same parity as k, where x_k is the known square. Note also that these bounds are larger than the threshold for (7) to apply. In sequence 3 it is easy to see that odd m's are impossible, by considering the sequence mod 8. Similarly, in sequence 4 even m's are impossible. For the other two sequences, no such simple resolution of the parity problem is possible, because both sequences begin with two squares in a row. The bounds for sequences 3 and 4 are small enough that it is quite feasible to eliminate the remaining m's by simple congruence arguments.

We now give a construction of an infinite family of examples of Theorem 1, for which the exponent ν improves steadily, approaching 1 in the limit. Let $w+u\sqrt{2}$ be a power of $1+\sqrt{2}$, so $w^2-2u^2=(-1)^u$. Let $dv^2=u^2+(-1)^u$, with d squarefree, and let $\varepsilon=u+v\sqrt{d}$. Consider the recurrence sequence $x_n=\mathrm{Tr}(\frac{1}{2}\varepsilon^n)$, with $x_0=1$, $x_1=u$, and $x_2=2u^2+(-1)^u=w^2$, a perfect square. For w moderately large, this gives a successful instance of

Theorem 1. For example, taking $w+u\sqrt{2} = 239+169\sqrt{2}$, with $\varepsilon = 169+4\sqrt{1785}$, one finds that $\nu < 1.4$. It is easy to see that $\sigma \to 0$ and $\nu \to 1$ as w increases. Many other infinite families may be constructed in this way. It should be noted in this connection that it is easy to build recurrence sequences with a specified large square in them; but unless this is done carefully, one has $x_n = \mathrm{Tr}(\alpha\varepsilon^n)$ with a bad value of α (or more precisely, of ζ, in the notation of Section 2).

4. In order to apply Theorem 1 to the problem of bounding the number of squares in a recurrence sequence, one needs a separation result on the occurrence of two squares. The author is grateful to the referee for pointing out the following lemma.

LEMMA 6. *Let $x_n = \mathrm{Tr}(\alpha\varepsilon^n)$, where $\varepsilon > 1$ is a unit in $Q(\sqrt{d})$ and $\alpha > 0$ is in $Q(\sqrt{d})$. Suppose that $x_k = x^2$ and $x_m = y^2$, where $m > k > 0$ and $m \equiv k \bmod 2$, and assume $\sigma < 1/2$ in (6). Let $\theta_k = \varepsilon^{2k}\alpha/|\bar{\alpha}|$ and $\theta_m = \varepsilon^{2m}\alpha/|\bar{\alpha}|$. Then*

$$\log\theta_m > 2\log\theta_k - \log 25|\alpha\bar{\alpha}|.$$

Proof. By Lemma 5, we have

$$\left|\frac{x}{\sqrt{\alpha}\varepsilon^{k/2}} - \frac{y}{\sqrt{\alpha}\varepsilon^{m/2}}\right| < \frac{|\bar{\alpha}|}{\alpha}\left(\frac{1}{\varepsilon^{2k}}+\frac{1}{\varepsilon^{2m}}\right) < \frac{2|\bar{\alpha}|}{\alpha\varepsilon^{2k}},$$

so

$$\left|\frac{x}{\varepsilon^{k/2}} - \frac{y}{\varepsilon^{m/2}}\right| < \frac{2|\bar{\alpha}|}{\sqrt{\alpha}\varepsilon^{2k}}. \tag{26}$$

Also,

$$\left|\frac{x}{\bar{\varepsilon}^{k/2}} - \frac{y}{\bar{\varepsilon}^{m/2}}\right| \leqslant |x\varepsilon^{k/2} + y\varepsilon^{m/2}| < 2y\varepsilon^{m/2} \leqslant 2\sqrt{\alpha}\varepsilon^m\sqrt{1+\frac{|\bar{\alpha}|}{\alpha\varepsilon^{2m}}}.$$

It is simple to check that $\sqrt{1+|\bar{\alpha}|/\alpha\varepsilon^{2m}} < 5/4$ since $m > k$ and $\sigma < 1/2$. Thus

$$\left|\frac{x}{\bar{\varepsilon}^{k/2}} - \frac{y}{\bar{\varepsilon}^{m/2}}\right| < \tfrac{5}{2}\sqrt{\alpha}\varepsilon^m. \tag{27}$$

If k and m are even, multiplication of (26) and (27) leads to

$$1 < 5|\bar{\alpha}|\varepsilon^{m-2k},$$

as the left-hand side is the product of two conjugate integers in $Q(\sqrt{d})$. If m and k are odd one obtains the same inequality by first factoring $\sqrt{\varepsilon}$ and $\sqrt{\bar{\varepsilon}}$ out of (26) and (27), and then multiplying. In either case, then,

$$\varepsilon^m > \varepsilon^{2k}/5|\bar{\alpha}|,$$

which may be rewritten as

$$\theta_m > \theta_k^2/25|\alpha\bar{\alpha}|$$

as the lemma asserts.

Roughly speaking, the content of Lemma 6 is that $m > 2k$; the inequality stated on θ_m and θ_k is more convenient to apply.

LEMMA 7. *Assume the situation in Theorem 1. Then $\nu < 1+\frac{7}{3}\sigma$.*

Proof. Let $\theta = \varepsilon^{2k}\zeta/|\zeta|$. From (6), we have

$$\theta^\sigma = 4^{3+4\sigma}3^{-(\frac{3}{4}+\frac{3}{2}\sigma)}(1+|z_0|)^{1+\sigma}N^{1+\sigma}.$$

Hence

$$\theta^{\sigma/3} \geqslant 4^{1+\frac{4}{3}\sigma}3^{-(\frac{1}{4}+\frac{1}{2}\sigma)}(1+|z_0|)^{(1+\sigma)/3},$$

and it is easy to see that in (8) $\nu < 1+\frac{7}{3}\sigma$.

The next theorem bounds the number of "large" squares in a recurrence sequence:

THEOREM 2. *Let $x_n = \mathrm{Tr}(\alpha\varepsilon^n)$ where $\varepsilon > 1$ is a unit in $Q(\sqrt{d})$ and $\alpha > 0$ is in $Q(\sqrt{d})$. Assume there is a series of s squares $x_{m_1}, x_{m_2}, \ldots, x_{m_s}$, where the m_i are positive, increasing, and of the same parity. Let σ_i and ν_i be the σ and ν for m_i in (6) and (8), and let $\theta_i = \varepsilon^{2m_i}\zeta/|\zeta|$. Assume $\sigma_1 < 1/2$ and $\log\theta_1 > 2\log 25|\alpha\bar{\alpha}|$. Then*

$$s < 3 + \frac{\log\left(14+\dfrac{\max(0,\ 21\log(|\bar{\alpha}|/\alpha))}{40\log 4 - 12\log 3 + 12\log N}\right)}{\log(9/5)}. \tag{28}$$

In particular, $s \leqslant 7$ if $|\bar{\alpha}| \leqslant \alpha$.

Note. 1. Here and subsquently φ and N have the same meaning as in Section 2: $\bar{\alpha}/\alpha = \pm\bar{\zeta}/\zeta$ with $\zeta > 0$ an algebraic integer, $N = |\zeta\bar{\zeta}|$, and $\varphi = \max\left(\dfrac{\zeta}{|\bar{\zeta}|}, \dfrac{|\bar{\zeta}|}{\zeta}\right)$.

2. The dependence on $|\bar{\alpha}|/\alpha$ in (28), if $|\bar{\alpha}| > \alpha$, is somewhat misleading: in this case, one may shift the sequence, replacing x_n by x_{n-t}, with $t \approx \frac{1}{2}\log(|\bar{\alpha}|/\alpha)/\log\varepsilon$. After this shift, one has $|\bar{\alpha}| \approx \alpha$. The "small" squares may have been shifted into the negative half of the sequence, but that is not the issue here. A careful analysis shows that the shift needed to make $|\bar{\alpha}| \leqslant \alpha$ will keep all the m_i positive except possibly m_1 (see (34) and (35)), thus showing that $s \leqslant 8$ in this case.

Proof. If $\nu < 2$ in Theorem 1 we have the upper bound (24) on m, which we may rewrite in terms of θ_m and θ_k as

$$\log\theta_m < \frac{5+\nu}{2-\nu}\log\theta_k + \frac{(3+2\nu)\log(|\bar{\alpha}|/\alpha) + 2\log C_1}{2-\nu}. \tag{29}$$

We are taking $\alpha = \beta$, so $\gamma = \eta = 1$ in (25). Thus we may write the numerator of the last term as C_2, where

$$C_2 = 2\nu\log(|\bar{\alpha}|/\alpha) + \log|\alpha\bar{\alpha}| + 4\log N + (\nu+1)\log\varphi + 9\log(1+|z_0|) + 50\log 2 - 10\log 3. \tag{30}$$

We will apply (29) with $k = m_i$ and $m = m_j, j > i$, and $v = v_i < 2$. If $|\bar{\alpha}| \leqslant \alpha$ then

$$2v\log\frac{|\bar{\alpha}|}{\alpha}+(v+1)\log\varphi = (v-1)\log\frac{|\bar{\alpha}|}{\alpha} \leqslant 0 \quad \text{as } v > 1.$$

If $\alpha < |\bar{\alpha}|$ the same two terms contribute $< 7\log(|\bar{\alpha}|/\alpha)$ in (30). By (6), since $\sigma_1 < 1/2$,

$$\theta_1 > \frac{4^{10}N^3}{3^3} \quad \text{and} \quad |z_0| \leqslant \frac{1}{\theta_1} < \frac{3^3}{4^{10}}.$$

Applying the inequalities above and $\theta_1 > 625(\alpha\bar{\alpha})^2$ from the hypotheses, we have

$$C_2-(\tfrac{4}{3}+\tfrac{1}{2})\log\theta_1 < \max(0, 7\log(|\bar{\alpha}|/\alpha))+\tfrac{70}{3}\log 2 -6\log 3-\log 25+9\log(1+|z_0|),$$

and thus

$$C_2 < \max(0, 7\log(|\bar{\alpha}|/\alpha))+\tfrac{5}{2}\log\theta_1. \tag{31}$$

Now write (29) in the form

$$\log\theta_j < \frac{5+v_i+\lambda_i}{2-v_i}\log\theta_i \tag{32}$$

where $\lambda_i = C_2/\log\theta_i$. Applying Lemma 6 successively,

$$\begin{aligned} \log\theta_2 &> 2\log\theta_1-\tfrac{1}{2}\log\theta_1 = \tfrac{3}{2}\log\theta_1,\\ \log\theta_3 &> \tfrac{5}{3}\log\theta_2 > \tfrac{5}{2}\log\theta_1, \qquad (33)\\ \log\theta_4 &> \tfrac{9}{5}\log\theta_3. \end{aligned}$$

Formula (6) for σ is of the form

$$\sigma = \frac{A}{\log\theta_k - B}$$

where $B = 4\log 4-\tfrac{3}{2}\log 3+\log(1+|z_0|)+\log N > 0$ certainly. Thus

$$\sigma_3 < \frac{A}{\tfrac{3}{2}\log\theta_1+(\log\theta_1-B)} < \tfrac{2}{5}\sigma_1 < \tfrac{1}{5}$$

using (33). Combining (32) and (33) we have

$$\left(\frac{9}{5}\right)^t\log\theta_3 < \log\theta_{3+t} < \frac{5+v_3+\lambda_3}{2-v_3}\log\theta_3,$$

which bounds s by

$$s < 3+\frac{\log\dfrac{5+v_3+\lambda_3}{2-v_3}}{\log\frac{9}{5}}.$$

By Lemma 7

$$v_3 < 1+\frac{7}{15}, \quad \text{and} \quad \lambda_3 < \frac{2C_2}{5\log\theta_1}$$

by (33), so

$$s < 3+\frac{\log\left(\dfrac{3C_2}{4\log\theta_1}+\dfrac{97}{8}\right)}{\log\frac{9}{5}}.$$

Finally, after using (31) one finds the bound (28) on s.

For Theorem 2 to apply we need $\sigma_1 < 1/2$ and $\theta_1 > 625(\alpha\bar{\alpha})^2$. These conditions translate to

$$m_1 > \frac{5\log 4-\tfrac{3}{2}\log 3+\log N+\log|\zeta|}{\log\varepsilon} \tag{34}$$

and

$$m_1 > \frac{2\log 5+\tfrac{1}{2}\log|\alpha\bar{\alpha}|+\log|\bar{\alpha}|}{\log\varepsilon}. \tag{35}$$

Each of these is of the form $m_1 > c_1+c_2\log H(\alpha)/\log\varepsilon$. Below these bounds the present method gives no information, and to bound the number of squares we have to assume that all terms in the recurrence sequence could be squares up to this point. Of course, with a specific value of α one can determine the bounds in (34) and (35) more explicitly. For example, if $\alpha = \pm\bar{\alpha}$ then $\zeta = 1$, and since $\varepsilon \geqslant (1+\sqrt{5})/2$, (34) is satisfied for $m_1 \geqslant 11$. If further $\alpha \leqslant 1$ then (35) also holds for $m_1 \geqslant 11$. Applying Theorem 2, such a sequence could have at most 25 squares x_n with $n \geqslant 0$. One could lower the bound to 15 for sufficiently large ε, as then (34) and (35) would require only that $m_1 \geqslant 1$.

5. We now present a generalization of Theorem 1 to the situation $x_n = \mathrm{Tr}(\alpha\theta^n)$, where θ is an algebraic integer, not necessarily a unit. Roughly speaking, the larger Norm θ is, the larger the initial square must be. For the sake of simplicity we take $\beta = \alpha$ and $\zeta = 1$, in the notation of Section 2.

THEOREM 3. *Let $x_n = \mathrm{Tr}(\alpha\theta^n)$, where α and θ are positive numbers in $\boldsymbol{Q}(\sqrt{d})$ such that θ is an algebraic integer, $|\bar{\theta}| < 1$, and $\alpha = \pm\bar{\alpha}$. For some $k \geqslant 1$, assume $x_k = x^2$, a perfect square in Z. Let $N = |\theta\bar{\theta}|$, $z_0 = -\bar{\alpha}\bar{\theta}^k/\alpha\theta^k$, and assume $\sigma < 1/2$, where*

$$\sigma = \frac{3\log 4-\tfrac{3}{4}\log 3+\log(1+|z_0|)+k\log N}{-2k\log|\bar{\theta}|+\tfrac{3}{2}\log 3-4\log 4-\log(1+|z_0|)}. \tag{36}$$

Let $y > 0$ and m be integers; assume m has the same parity as k, and

$$m \geqslant k\cdot\left(1+\frac{1}{\sigma}\cdot\frac{\alpha^2}{2^9}\right). \tag{37}$$

Define v by

$$v = 1+2\sigma+\frac{(1+2\sigma)\log 4-(\frac{3}{4}+\frac{3}{2}\sigma)\log 3+\sigma\log(1+|z_0|)}{k\log(\theta/|\bar{\theta}|)}. \tag{38}$$

Then

$$\left|\frac{y}{\sqrt{\alpha}\theta^{m/2}}-1\right| > C\cdot\left(\frac{\theta}{|\bar{\theta}|}\right)^{-mv/2},$$

where

$$C = \frac{3^5 N^{kv/2}}{2^{25}\alpha(1+|z_0|)^{9/2}\theta^{k(5+v)}}.$$

Proof. We proceed as in the proof of Theorem 1. We have

$$\binom{n}{n_1}G(z_0) = \frac{A}{(4\theta^k)^{n_1}} \quad \text{and} \quad \binom{n}{n_1}H(z_0) = \frac{B}{(4\theta^k)^{n_2}}$$

for algebraic integers A and B in $\boldsymbol{Q}(\sqrt{d})$. From (2) of Lemma 1,

$$\left|1-\frac{xB}{\sqrt{\alpha}\theta^{k/2}A(4\theta^k)^{\lambda}}\right| < \frac{\binom{n}{n_1}G(1)|\bar{\theta}|^k}{\theta^k}\cdot\frac{4^{n_1}|\bar{\theta}|^{kn}}{|A|\theta^{kn_2}}$$

where $\lambda = n_2-n_1$ as before. Add to $\delta = |y/\sqrt{\alpha}\theta^{m/2}-1|$ to get

$$\left|\frac{y}{\sqrt{\alpha}\theta^{m/2}}-\frac{xB}{\sqrt{\alpha}\theta^{k/2}A(4\theta^k)^{\lambda}}\right| < \delta+\frac{\binom{n}{n_1}G(1)|\bar{\theta}|^k}{\theta^k}\cdot\frac{4^{n_1}|\bar{\theta}|^{kn}}{|A|\theta^{kn_2}}. \tag{39}$$

We choose λ to be the nearest integer to $m/2k$, so

$$m/2k = \lambda+\mu, \qquad -1/2 < \mu \leqslant 1/2.$$

The second term of the left side of (39) has the higher power of θ, so the fraction may be written as

$$\frac{yA4^{\lambda}\theta^{k\lambda+(k-m)/2}-xB}{\sqrt{\alpha}A4^{\lambda}\theta^{k/2+k\lambda}}. \tag{40}$$

Let K be the numerator above; K is an algebraic integer in $\boldsymbol{Q}(\sqrt{d})$. We select n_1 so that

$$\sigma\lambda \leqslant n_1 < \sigma\lambda+2,$$

as before, so $K \neq 0$ for at least one choice of n_1. Thus $|K| \geqslant |\bar{K}|^{-1}$. Now,

$$|\bar{A}| = \binom{n}{n_1}4^{n_1}|\bar{\theta}|^{kn_1}|G(\bar{z}_0)| < \binom{n}{n_1}4^{n_1}\theta^{kn_1}(1+|z_0|)^{n_1}$$

by Lemma 2, and similarly

$$|\bar{B}| < \binom{n}{n_1}4^{n_2}\theta^{kn_2}(1+|z_0|)^{n_2}.$$

Without loss we may assume $\delta < 1$, so $y < 2\sqrt{\alpha}\theta^{m/2}$. Also,

$$x = \sqrt{\alpha\theta^k+\bar{\alpha}\bar{\theta}^k} \leqslant \sqrt{\alpha}\theta^{k/2}\sqrt{1+|z_0|},$$

giving an estimate on $\bar{K}$ as

$$\begin{aligned}|\bar{K}| &< 2\sqrt{\alpha}\theta^{m/2}\binom{n}{n_1}4^{n_2}\theta^{kn_1}(1+|z_0|)^{n_1}|\bar{\theta}|^{k\lambda+(k-m)/2}\\ &\quad+\sqrt{\alpha}\theta^{k/2}\binom{n}{n_1}4^{n_2}\theta^{kn_2}(1+|z_0|)^{n_2+1/2}\\ &< 3\sqrt{\alpha}\binom{n}{n_1}4^{n_2}\theta^{k/2}(1+|z_0|)^{n_2+1/2}\theta^{kn_2}.\end{aligned}$$

This combines with (39) and (40) to give

$$1 < \delta L+\left(\binom{n}{n_1}G(1)|\bar{\theta}|^k 3\alpha\sqrt{1+|z_0|}\right)\left(4^{2n_2}\binom{n}{n_1}\theta^{k\lambda}|\bar{\theta}|^{kn}(1+|z_0|)^{n_2}\right), \tag{41}$$

where

$$L = 3\alpha\theta^k\binom{n}{n_1}4^{n_2+\lambda}|A|(1+|z_0|)^{n_2+1/2}\theta^{k(n_2+\lambda)}.$$

Here we see that the condition $|\bar{\theta}| < 1$ is essential; otherwise, the second term on the right side of (41) would be exponentially growing rather than decreasing. We have $n \geqslant 4n_1-3$ as before, so the second parenthesis in (41) is less than

$$\begin{aligned}&4^{2n_1+2\lambda}\left(\frac{4}{3^{3/4}}\right)^{2n_1+\lambda}(1+|z_0|)^{n_1+\lambda}N^{k\lambda}|\bar{\theta}|^{2kn_1}\\ &\qquad\leqslant\left[4^{2+2/\sigma}\left(\frac{4}{3^{3/4}}\right)^{2+1/\sigma}(1+|z_0|)^{1+1/\sigma}N^{k/\sigma}|\bar{\theta}|^{2k}\right]^{n_1}.\end{aligned}$$

This is 1 by (36). Since $\sigma < 1/2$, (36) implies that

$$|\bar{\theta}|^{-k} \geqslant \frac{2^{10}}{3^{3/2}}(1+|z_0|)^{3/2}N^k.$$

By Lemma 3 and (37) it follows that the second term on the right of (41) is less than 1/2. Hence

$$\delta > \frac{1}{2L} = \left[6\alpha\theta^k\binom{n}{n_1}4^{n_2+\lambda}|A|(1+|z_0|)^{n_2+1/2}\theta^{k(n_2+\lambda)}\right]^{-1}. \tag{42}$$

Since

$$|A| = \binom{n}{n_1}(4\theta^k)^{n_1}|G(z_0)| < \binom{n}{n_1}(4\theta^k)^{n_1}(1+|z_0|)^{n_1},$$

by Lemma 4 we have the bracket above bounded by

$$(6\alpha\theta^k\sqrt{1+|z_0|})\left(4^{2n_2}\left(\frac{4}{3^{3/4}}\right)^{2n}(1+|z_0|)^n\theta^{2kn_2}\right). \tag{43}$$

The second factor of (43) is

$$4^{2n_1+2\lambda}\left(\frac{4}{3^{3/4}}\right)^{4n_1+2\lambda}(1+|z_0|)^{2n_1+\lambda}N^{k(n_1+\lambda)}\left(\frac{\theta}{|\bar\theta|}\right)^{k(n_1+\lambda)}$$
$$\leqslant\left[4^{2+2\sigma}\left(\frac{4}{3^{3/4}}\right)^{2+4\sigma}(1+|z_0|)^{1+2\sigma}N^{k(1+\sigma)}\left(\frac{\theta}{|\bar\theta|}\right)^{k(1+\sigma)}\right]^{\lambda}$$
$$\times\left[4^2\left(\frac{4}{3^{3/4}}\right)^4(1+|z_0|)^2N^k\left(\frac{\theta}{|\bar\theta|}\right)^k\right]^2.$$

The first bracket is $(\theta/|\bar\theta|)^{k\lambda\nu}$ by the definition of ν. Finally,

$$\left(\frac{\theta}{|\bar\theta|}\right)^{k\lambda\nu} = \left(\frac{\theta}{|\bar\theta|}\right)^{\nu(m/2-k\mu)} \leqslant \left(\frac{\theta}{|\bar\theta|}\right)^{\nu((m+k)/2)},$$

and combining the above with (42) and (43) completes the proof.

Note that the analog of Lemma 5 for $x_n = \mathrm{Tr}(\alpha\theta^n)$ is that if $x_n = x^2$, then

$$\left|\frac{x}{\sqrt{\alpha}\theta^{n/2}} - 1\right| < \frac{|\bar\alpha|}{\alpha}\left(\frac{|\bar\theta|}{\theta}\right)^n,$$

so it is appropriate to give the lower bound for δ as a power of $\theta/|\bar\theta|$ rather than of θ. A successful example of Theorem 3 is provided by the sequence $x_n = \mathrm{Tr}(\frac{1}{2}\theta^n)$ with $\theta = 41+3\sqrt{187}$ and $N = 2$. Here $x_2 = 3364 = 58^2$, $\sigma = .4308$, and $\nu = 1.9261$. This example is in fact one of an infinite family constructed similarly to the one given in Section 3.

Note also that the method of Theorem 3 does not apply in an imaginary quadratic field since then the condition $|\bar\theta| < 1$ obviously cannot be fulfilled.

The method of Lemma 6 applies in the situation of Theorem 3 to give a similar separation result:

LEMMA 8. *Let $x_n = \mathrm{Tr}(\alpha\theta^n)$ where α and θ are positive numbers in $Q(\sqrt{d})$, θ is an algebraic integer, $|\bar\theta| < 1$, and $\alpha = \pm\bar\alpha$. Let $N = |\theta\bar\theta|$, and $\tau = \log N/\log\theta$. Suppose that $x_k = x^2$ and $x_m = y^2$, where $m > k > 0$ and $m \equiv k \bmod 2$. Then*

$$m > (2-\tau)k - \frac{\log 4\sqrt{2\alpha}}{\log\theta}.$$

Proof. Proceeding as in Lemma 6, we have

$$\left|\frac{x}{\theta^{k/2}} - \frac{y}{\theta^{m/2}}\right| < \frac{2\sqrt{\alpha}N^k}{\theta^{2k}} \tag{44}$$

and

$$\left|\frac{x}{\bar\theta^{k/2}} - \frac{y}{\bar\theta^{m/2}}\right| < \frac{2\sqrt{2\alpha}\theta^m}{N^{m/2}}. \tag{45}$$

Multiplying these, we have

$$\frac{1}{N^{m/2}} < \frac{4\sqrt{2}\alpha\theta^{m-2k}N^k}{N^{m/2}},$$

which implies the inequality of the lemma.

As $|\bar\theta| < 1$, $\tau < 1$ and the lemma provides an effective separation of m and k.

References

[1] A. Baker and J. Coates, *Integer points on curves of genus 1*, Proc. Cambr. Phil. Soc. 67 (1970), 595–602.

[2] F. Beukers, *On the generalized Ramanujan–Nagell equation I*, Acta Arith. 38 (1981), 389–410.

[3] J. H. E. Cohn, *Lucas and Fibonacci numbers and some diophantine equations*, Proc. Glasgow Math. Assoc. 7 (1965), 24–28.

[4] W. J. Ellison *et al.*, *The diophantine equation $y^2+k = x^3$*, J. Number Theory 4 (1972), 107–117.

[5] J. H. Evertse, *On equations in S-units and the Thue–Mahler equation*, Inv. Math. 75 (1984), 561–584.

[6] W. Ljunggren, *Über die unbestimmte Gleichung $Ax^2 - By^4 = C$*, Archiv for Math. Naturv. 41 (1938), no. 10.

[7] A. Pethő, *Perfect powers in second order linear recurrences*, J. Number Theory 15 (1982), 5–13.

[8] T. N. Shorey and C. L. Stewart, *On the diophantine equation $ax^{2t}+bx^ty+cy^2 = d$ and pure powers in recurrence sequences*, Math. Scand. 52 (1983), 24–36.

[9] — — *Pure powers in recurrence sequences and some related diophantine equations*, J. Number Theory 27 (1987), 324–352.

[10] T. N. Shorey and R. Tijdeman, *Exponential diophantine equations*, Cambridge University Press, 1986.

[11] N. Tzanakis, *On the diophantine equation $y^2-D = 2^k$*, J. Number Theory 17 (1983), 144–164.

STATE UNIVERSITY OF NEW YORK AT BUFFALO
Buffalo, New York 14214
and
NORTHERN ILLINOIS UNIVERSITY
DeKalb, Illinois 60115

Received on 27.7.1987
and in revised form on 26.5.1988 (1737)