GLASNIK MATEMATIČKI
Vol. 38(58)(2003), 11 – 18

NEAR SQUARES IN LINEAR RECURRENCE SEQUENCES

P. G. Walsh
University of Ottawa, Canada

Abstract. Let $T > 1$ denote a positive integer. Let $\{U_n\}$ denote the linear recurrence sequence defined by $U_0 = 0$, $U_1 = 1$, and $U_{k+1} = 2TU_k - U_{k-1}$ for $k \geq 1$. In recent years there have been some improvements on the determination of solutions to the Diophantine equation $U_n = cX^2$, where c is a given positive integer. In this paper we use a result of Bennett and the author to determine precisely the integer solutions to the related equation $U_n = cx^2 \pm 1$, where c is a given even positive integer.

1. Introduction

Let r, s, U_0, U_1 denote integers. The relation

$$U_{n+1} = rU_n - sU_{n-1} \tag{1}$$

defines a binary linear recurrence sequence $\{U_n\}$ for $n \geq 1$. For a polynomial $P(x)$ of degree at least two with integer coefficients, Nemes and Pethö [16] described necessary conditions for the general equation

$$U_n = P(x) \tag{2}$$

to have infinitely many solutions in integers (n, x). In the particular case $P(x) = bx^2$, for $b \geq 1$, precise results on the solutions of (2) have been obtained by Ljunggren [11, 9, 12, 13, 10], Cohn [5], McDaniel and Ribenboim [14, 15], Shorey and Stewart [18], Bennett and the author [4], and a host of others. For a comprehensive survey on these results the reader is referred to [22].

In the case that $P(x)$ is quadratic and the sequence in question is of Lucas-Lehmer type, there exist methods to determine all solutions. The method of

2000 *Mathematics Subject Classification.* 11D25, 11B39.
Key words and phrases. Linear recurrence sequence, diophantine equation, Pell equation.

Baker [1] provides an explicit upper bound for the size of solutions to (2). In [20], Tzanakis describes an algorithmic approach to determine all solutions to (2). It is our interest to determine families of such equations for which one can make explicit statements of solvability. In the present paper we consider the particular case that $P(x) = cx^2 \pm 1$ for an even positive integer c, and for which the linear recurrence sequence defined in (1) is given by $(r, s, U_0, U_1) = (2T, 1, 0, 1)$, for some positive integer $T > 1$. Similar problems were considered by Robbins in [17].

Let $T > 1$ denote a positive integer, and define $\alpha = T + \sqrt{T^2 - 1}$. For $n \geq 1$, define sequences $\{T_n\}$ and $\{U_n\}$ by

$$\alpha^n = T_n + U_n\sqrt{T^2 - 1}.$$

Also, for $i \geq 1$, define sequences $\{p_i\}$, $\{q_i\}$ by

$$p_i + q_i\sqrt{2} = (1 + \sqrt{2})^i.$$

Employing a technique of Ljunggren's in [9], developed further in work of Cohn [7], together with results in [4, 6], we prove the following result.

Theorem 1.1.

1. *If $(T, c) = (q_{2i+1}, 2)$ for some $i \geq 1$, then the equation*

$$U_n = cx^2 \pm 1$$

   has only the two positive integer solutions $(n, x) = (1, 1), (3, p_{2i+1})$.

2. *If (T, c) is any other pair of positive integers for which $T > 1$ and c is even, then the equation*

$$U_n = cx^2 \pm 1$$

   has only one solution in positive integers (n, x), and if a solution exists, then $n < c$.

The proof of this theorem will appear to be of an elementary nature, but the reader should be made aware that it relies on the main result of [4], whose proof is based on estimates for linear forms in two logarithms of algebraic numbers, together with sharp gap results from diophantine approximation stemming from work of Bennett in [2, 3].

2. Preliminary Results

Let $d > 1$ denote a positive nonsquare integer, let $(X, Y) = (t_1, u_1)$ be the smallest solution in positive integers to the equation $X^2 - dY^2 = 1$, define $\epsilon_d = t_1 + u_1\sqrt{d}$, and for $n \geq 1$, $t_n + u_n\sqrt{d} = \epsilon_d^n$.

Definition 2.1. *For a positive integer b, the* rank of apparition *$\beta(b)$ of b in the sequence $\{t_n\}$ is the minimal index n for which b divides t_n. We write $\beta(b) = \infty$ if no such n exists.*

In the following result we record some basic results about the sequences $\{t_n\}$ and $\{u_n\}$ which will be required for our proof of Theorem 1.1. The proofs can be found in Lehmer's seminal paper [8].

Lemma 2.2.

1. $(t_n, u_n) = 1$.
2. $t_{2n} = 2u_n^2 - 1$, $u_{2n} = 2t_n u_n$.
3. $(t_n, u_{n+1}) = 1$ *if* n *is even, and* $(t_n, u_{n+1}) = t_1$ *if* n *is odd.*
4. *If* $b > 1$, *then* b *divides* u_n *with* n *odd if and only if* $\beta(b) = \infty$.
5. *If* $b > 1$ *and* $\beta(b) < \infty$, *then* b *divides* t_m *if and only if* $m/\beta(b)$ *is an odd integer.*
6. *If a prime* p *divides* t_m *for some odd integer* m, *then* p *does not divide* t_n *for any even integer* n.
7. t_n *is odd for all* n *even.*
8. *If* 2^μ $(\mu \geq 0)$ *properly divides* t_1, *then* 2^μ *properly divides* t_n *for all odd* n.
9. *If* p *is an odd prime for which* $\beta(p) < \infty$, *then* $\beta(p)$ *divides one of* $(p \pm 1)/4$.

The following result will be used considerably during the course of proving Theorem 1.1. The first part was proved by Cohn in [6], extending classical work of Ljunggren [11], while the latter part is the main result of Bennett and the author in [4].

Lemma 2.3. *If* $t_n = x^2$ *for some integer* x, *then* $n = 1$ *or* $n = 2$. *If* $b > 1$ *is squarefree, and* $t_n = bx^2$ *for some integer* x, *then* $n = \beta(b)$.

We will also make use of the following result, which follows immediately from the main result of [21], which itself was an extension of a classical result of Ljunggren [9].

Lemma 2.4. *If there are* 2 *indices* $i < j$ *for which* u_i *and* u_j *are squares, then* $i = 1$ *and* $j = 2$, *except only for* $d \in \{1785, 28560\}$, *in which case* u_1 *and* u_4 *are squares.*

As an immediate consequence of Lemma 2.4, we record the following.

Corollary 2.5. *If* i *and* j *are odd positive integers for which* $u_i u_j$ *is a square, then* $i = j$.

3. Proof of Theorem 1.1

We will first show that there is at most one solution (n, x) in positive integers to

$$U_n = cx^2 - 1. \tag{3}$$

Suppose that (n, x) and (m, z) are positive integer solutions to (3). Since c is even, n and m must be odd. Let $n = 2k+1$ and $m = 2l+1$ for non-negative integers k and l. The relation

$$T_{2k+1} + U_{2k+1}\sqrt{T^2-1} = (T + \sqrt{T^2-1})(T_{2k} + U_{2k}\sqrt{T^2-1}),$$

together with part 2 of Lemma 2.2, show that

$$U_n = U_{2k+1} = T_{2k} + TU_{2k} = 2T_k^2 - 1 + 2TT_kU_k,$$

and hence (3) implies that

$$(c/2)x^2 = T_k(T_k + TU_k) = T_kU_{k+1}. \tag{4}$$

Similarly,

$$(c/2)z^2 = T_lU_{l+1}. \tag{5}$$

Let $c/2 = CD^2$, where $C \geq 1$ is a squarefree integer.

Assume first that k and l are even. Then since T_k and U_{k+1} are coprime, there are integers A, B, w, v, with $C = AB$, for which

$$T_k = Aw^2,\ U_{k+1} = Bv^2.$$

Similarly, there are integers a, b, W, V, with $C = ab$, such that

$$T_l = aW^2,\ U_{l+1} = bV^2.$$

Since $k+1$ and $l+1$ are odd, $\beta(p) = \infty$ for each prime dividing B and b. Moreover, $\beta(p) < \infty$ for each prime dividing a and A. Since $AB = ab$, it follows that $a = A$. By Lemma 2.3, either $A = a = 1$ and $k = l = 2$, or $A = a > 1$ and $k = \beta(A) = \beta(a) = l$. In any case we have that $k = l$, forcing $(n, x) = (m, z)$.

Assume now that k and l are odd. By part 3 of Lemma 2.2, equations (4) and (5) imply the existence of integers A, B, w, v, a, b, W, V, with $C = AB = ab$, for which

$$T_k = T_1Aw^2,\ U_{k+1} = T_1Bv^2,\ \ T_l = T_1aW^2,\ U_{l+1} = T_1bV^2. \tag{6}$$

Let $r = \mathrm{ord}_2(k+1)$ and $s = \mathrm{ord}_2(l+1)$, then

$$U_{k+1} = 2^rT_{(k+1)/2}\cdots T_{(k+1)/2^r}U_{(k+1)/2^r} = T_1Bv^2 \tag{7}$$

and

$$U_{l+1} = 2^sT_{(l+1)/2}\cdots T_{(l+1)/2^s}U_{(l+1)/2^s} = T_1bV^2. \tag{8}$$

We will show that $r = s$. Assume that $s > r$. Let p be a prime dividing b for which p divides $T_{(l+1)/2}$. By part 5 of Lemma 2.2, $\beta(p)$ is divisible by 2^{s-1}. Equation (6) shows that $\beta(q)$ is odd for each prime q dividing A, and our assumption that $s > r$ together with equation (7) shows that $\mathrm{ord}_2(\beta(q)) < s-1$ for each prime q dividing B. Therefore, $T_{(l+1)/2}$ is coprime to b. Since the factors appearing in (8) are pairwise coprime, and $(T_1, T_{(l+1)/2}) = 1$, we deduce that $T_{(l+1)/2} = Y^2$ for some integer Y. By Lemma 2.3, it follows that $(l+1)/2 = 2$, and hence that $l+1 = 4$. By our assumption on r and s, $k+1 = 2k_1$ for some odd integer k_1. Part 7 of Lemma 2.2 shows that A and a are odd integers. Since $k+1$ is properly divisible by 2 and $l+1$ is properly divisible by 4, equation (6) implies that $\operatorname{ord}_2(ab) > \operatorname{ord}_2(AB)$, a contradiction. As the argument is symmetric in r and s, we conclude that $r = s$.

Let $c/2 = fg$, where a prime p divides f if $\beta(p) = \infty$, and p divides g otherwise. It follows from equations (6), (7), (8), and the fact that $s = r$, that there are integers Y, Z such that

$$U_{(l+1)/2^r} = fY^2,\ U_{(k+1)/2^r} = fZ^2.$$

By Corollary 2.5, it follows that $l = k$.

Assume now that k is even and l is odd. As before there are integers A, B, w, v, a, b, W, V, with $C = AB = ab$, such that

$$T_k = Aw^2,\ U_{k+1} = Bv^2,\ T_l = T_1 aW^2,\ U_{l+1} = T_1 bV^2.$$

Note that A and B are odd in this case. As $(T_k, T_l) = 1$, we have that A divides b. Since $\beta(p) = \infty$ for all primes p dividing B, it follows that B divides b. Therefore $a = 1$, and $T_l/T = W^2$, which by Lemma 2.3 implies that $l = 1$. Therefore, $T_1 bV^2 = U_{l+1} = U_2 = 2T_1U_1 = 2T_1$, and hence $AB = ab = 2$, contradicting the fact that A and B are odd.

Now suppose that (n, x) is a positive integer solution to

$$U_n = cx^2 + 1. \tag{9}$$

The integer n is evidently odd, so let $n = 2k+1$ for some integer $k \geq 1$ (if $k = 0$, then $x = 0$, which we rule out). From the relation

$$U_n = U_{2k+1} = T_1U_{2k+2} - T_{2k+2} = 2T_1T_{k+1}U_{k+1} - (2T_{k+1}^2 - 1),$$

it follows that

$$(c/2)x^2 = T_{k+1}(T_1U_{k+1} - T_{k+1}) = T_{k+1}U_k,$$

and the argument proceeds in a manner similar to the previous case. We forego the details.

Now assume that (n, x) is a positive integer solution to (3), and that (m, z) is a positive integer solution to (9). We must show that there is an index i for which $(T, c) = (q_{2i+1}, 2)$, $(n, x) = (1, 1)$, and $(m, z) = (3, p_{2i+1})$, where p_i, q_i were defined above.

As before, n and m are odd positive integers, so let k and l be non-negative integers for which $n = 2k+1$ and $m = 2l+1$. As in equation (4), we see that

$$(c/2)x^2 = T_kU_{k+1},\ (c/2)z^2 = T_{l+1}U_l. \tag{10}$$

Consider first the case that k and l are odd. If $k = 1$, then $(c/2)x^2 = T_1U_2 = 2T_1^2$, and so $T_{l+1}U_l = 2w^2$ for some integer w. This is not possible because U_l and T_{l+1} are both odd. If $k > 1$, then $T_k = Aw^2$ for some squarefree integer $A > 1$, and integer w. Let p be a prime factor of A, then $\beta(p)$ is odd. Also, since $(T_k, U_{k+1}) = 1$, p divides $c/2$, and so p divides one of T_{l+1} or U_l. If p divides T_{l+1}, then $\beta(p)$ is even, while if p divides U_l, then $\beta(p) = \infty$.

Assume now that k and $l > 0$ are even. Since $z > 0$, $l \geq 1$, and so $T_{l+1} = Aw^2$ for some squarefree integer $A > 1$, and integer w. If p divides A, then $\beta(p)$ is odd, while as argued in the previous paragraph, p must divide $c/2$, forcing p to divide one of T_k or U_{k+1}. It follows that either $\beta(p)$ is even, or $\beta(p) = \infty$, a contradiction.

Assume now that k is odd and $l > 0$ is even. Assume first that $T_{(k+1)/2}$ and $T_{l/2}$ are nonsquare integers. We first show that $(k+1)/2$ and $l/2$ are of the same parity. Assume that $(k+1)/2$ is even. Since $T_{(k+1)/2}$ divides the product $T_k U_{k+1}$ in (10), there is at least one prime p dividing $T_k U_{k+1}$ to an odd power for which $\beta(p)$ is even. Therefore, p divides $T_{l+1}U_l = 2T_{l+1}T_{l/2}U_{l/2}$, and hence p divides $T_{l/2^r}$ for some positive integer r. The point is that $l/2$ must also be even, and by symmetry, it follows that $(k + 1)/2$ and $l/2$ are of the same parity. If $(k + 1)/2$ and $l/2$ are both odd, then as argued in an earlier case, $U_{(k+1)/2} = fY^2$, $U_{l/2} = fZ^2$ for some integer f, which implies that $k+1 = l$. Therefore, (10) shows that $(c/2)x^2 = T_k U_{k+1}$ and $(c/2)z^2 = T_{k+2}U_{k+1}$, from which we deduce that $T_k T_{k+2}$ is a square, which is not possible by Lemma 2.3. If $(k+1)/2$ and $l/2$ are even, then as argued in an earlier case, $T_{(k+1)/2} = fX^2$ and $T_{l/2} = fY^2$ for some squarefree integer $f > 1$. Lemma 2.3 shows that $k + 1 = l$, and so a contradiction is derived as before. If $T_{(k+1)/2}$ and $T_{l/2}$ are squares, then $k = 1$ or $k = 3$, and $l = 2$ or $l = 4$. If $k = 1$, then $(c/2)x^2 = T_1U_2 = 2T_1^2$. If $l = 2$, then $T_3U_2 = 2z^2$ for some integer z, and it follows that T_3/T_1 is a square, which is not possible. If $l = 4$, then in the same way it follows that T_5/T_1 is a square, which is also not possible. If $k = 3$ and $l = 2$, then $(c/2)x^2 = T_3U_4$ and $(c/2)z^2 = T_3U_2$, forcing $U_4/U_2 = 2T_2$ to be a square, which is not possible because T_2 is odd. If $k = 3$ and $l = 4$, then $(c/2)x^2 = T_3U_4$ and $(c/2)z^2 = T_5U_4$, which shows that T_5T_3 must be a square, contradicting Lemma 2.3.

Assume that k is even and l is odd. As argued before, there are integers f, X, Y for which $U_{k+1} = fX^2$ and $U_l = fY^2$, from which it follows that $k + 1 = l$. Also, if T_k and T_{l+1} are not squares, there is are integers $f_1 > 1, X_1, Y_1$ for which $T_k = f_1X_1^2$ and $T_{l+1} = f_1Y_1^2$, from which it follows that $k = l + 1$, contradicting $k + 1 = l$. Therefore, T_k and T_{l+1} are squares. Since l is odd, $l + 1 = 2$ by Lemma 2.3, and hence $(k, l) = (0, 1)$. This shows that $n = 1$, $x = 1$, $c = 2$, and $m = 3$. Furthermore, the relation $(c/2)z^2 = T_{l+1}U_l$ becomes $z^2 = T_2 = 2T_1^2 - 1$, and so $(z, T_1) = (p_{2i+1}, q_{2i+1})$ for some integer $i \geq 1$.

We now prove the last part of the statement of Theorem 1.1. Let (n, x) be a solution to (3), with $n = 2k + 1$ for some integer k, and assume that $n \geq c$. As shown in the argument proving that only one solution to (3) exists, either $k = 1$, $k = 2$, or $k = \beta(A)$ for some squarefree integer $A > 1$ which divides $c/2$, and is divisible by at least one odd prime. If $k = 1$, then $n = 3$, $c = 2$, and (4) shows that $x^2 = T_1U_2 = T_1(2T_1U_1) = 2T_1^2$, which is clearly not possible. If $k = 2$, then $n = 5$ and $c \in \{2, 4\}$. Therefore, by (4), we have that $2^\delta x^2 = T_2U_3$, where $\delta \in \{0, 1\}$. Since $(T_2, U_3) = 1$ and U_3 is odd, U_3 must be a square, contradicting Corollary 2.5. Finally, assume that $k = \beta(A)$, where A is squarefree and divisible by an odd prime p. Then

$$n \le 2\beta(A) + 1 \le 2\left(\prod_{p|A} \beta(p)\right) + 1 \le 2\left(\prod_{p|(c/2)} ((p+1)/4)\right) + 1 \le c/2 < c.$$

If (n, x) is a solution to (9), with $n = 2k + 1$, then a similar argument as that for a solution to (3) shows that either $k+1 = 1$, $k+1 = 2$, or $k+1 = \beta(A)$ for some squarefree integer $A > 1$, which divides $c/2$, and is divisible by at least one odd prime. In the case that $k + 1 = \beta(A)$, the condition $n \ge c$ is ruled out in exactly the same manner as the case $k = \beta(A)$ was dealt with in the previous paragraph. If $k + 1 = 1$, then $n = 1$, and so $n < c$. Finally, if $k+1 = 2$, then $n = 3$. The condition $n \ge c$ implies that $c = 2$. Therefore, (5) shows that

$$x^2 = T_2U_1 = T_2 = 2T_1^2 - 1,$$

which shows that we are in the situation of the first part of the statement of Theorem 1.1.

References

[1] A. Baker, *Bounds for the solutions of the hyperelliptic equation*, Proc. Camb. Phil. Soc. **65** (1969), 439–444.

[2] M.A. Bennett, *On the number of solutions to simultaneous Pell equations*, J. Reine Angew. Math. **498** (1998), 173–200.

[3] M.A. Bennett, *On consecutive integers of the form* ax^2, by^2, cz^2, Acta Arith. **88** (1999), 363–370.

[4] M.A. Bennett and P.G. Walsh, *The Diophantine equation* $b^2X^4 - dY^2 = 1$, Proc. Amer. Math. Soc. **127** (1999), 3481–3491.

[5] J.H.E. Cohn, *On square Fibonacci numbers*, J. London Math. Soc. **39** (1964), 537–541.

[6] J.H.E. Cohn, *The Diophantine equation* $x^4 - Dy^2 = 1$ *II*, Acta Arith. **78** (1997), 401–403.

[7] J.H.E. Cohn, *The Diophantine system* $x^2 - 6y^2 = -5, x = 2z^2 - 1$, Math. Scand. **82** (1998), 161–164.

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

[9] W. Ljunggren, *Einige Eigenschaften der Einheiten reeller quadratischer und reinbiquadratischer Zahl-Körper mit Anwendung auf die Lösung einer Klasse unbestimmter Gleichungen vierten Grades*, Oslo Vid.-Akad. Skrifter nr. 12, (1936), 1–73.

[10] W. Ljunggren, *Über die unbestimmte Gleichung* $Ax^2 - By^4 = C$, Arch. Math. Naturvid. **41** no. 10 (1938), 1–18.

[11] W. Ljunggren, *Über die Gleichung* $x^4 - Dy^2 = 1$, Arch. Math. Naturvid. **45** no. 5 (1942), 1–12.

[12] W. Ljunggren, *Ein Satz über die Diophantische Gleichung* $Ax^2 - By^4 = C$ $(C = 1, 2, 4)$, Tolfte Skand. Matemheikerkongressen, Lund, 1953, 188–194, (1954).
[13] W. Ljunggren, *On the Diophantine equation* $Ax^4 - By^2 = C(C = 1, 4)$, Math. Scand. **21** (1967), 149–158.
[14] W.L. McDaniel and P. Ribenboim, *Squares and double squares in Lucas sequences*, C.R. Math. Rep. Acad. Sci. Canada **14** (1992), 104–108.
[15] W.L. McDaniel and P. Ribenboim, *The square terms in Lucas sequences*, J. Number Theory **58** (1996), 104–123.
[16] I. Nemes and A. Pethö, *Polynomial values in linear recurrence sequences II*, J. Number Theory **24** (1986), 47–53.
[17] N. Robbins, *On Fibonacci and Lucas numbers of the forms* $w^2 - 1, w^3 \pm 1$, Fibonacci Quart. **19** (1981), 369–373.
[18] T.N. Shorey and C.L. Stewart, *On the diophantine equation* $ax^{2t} + bx^t y + cy^2 = d$, Math. Scand. **52** (1983), 24–36.
[19] T.N. Shorey and R. Tijdeman, Exponential Diophantine Equations, Cambridge University Press, **87**, New York, 1986.
[20] N. Tzanakis, *Solving elliptic Diophantine equations by estimating linear forms in elliptic logarithms. The case of quartic equations*, Acta Arith. **75** (1996), no. 2, 165–190.
[21] P.G. Walsh, *A note on a theorem of Ljunggren and the Diophantine equations* $x^2 - kxy^2 + y^4 = 1, 4$, Arch. Math. **72** (1999), 1–7.
[22] P.G. Walsh, *Diophantine equations of the form* $aX^4 - bY^2 = \pm 1$, in: Algebraic Number Theory and Diophantine Analysis, Proceedings of a conference in Graz 1998, F. Halter-Koch and R. Tichy, Eds. de Gruyter Proceedings in Mathematics, de Gruyter, 2000.

P.G. Walsh
Department of Mathematics
University of Ottawa
585 King Edward St.
Ottawa, Ontario, Canada
K1N-6N5

E-mail: gwalsh@mathstat.uottawa.ca

Received: 01.07.2002.
Revised: 15.09.2002.