manuscripta math. 96, 195 – 202 (1998)

Takaaki Kagawa · Nobuhiro Terai

Squares in Lucas sequences and some Diophantine equations

Received: 8 November 1996 / Revised version: 4 December 1997

1. Introduction

Let P and Q be non-zero relatively prime integers. The Lucas sequence $\{U_n\}$ and the companion Lucas sequence $\{V_n\}$ with parameters P and Q are defined as follows:

$$U_0 = 0, \quad U_1 = 1, \quad U_{n+2} = PU_{n+1} - QU_n,$$
$$V_0 = 2, \quad V_1 = P, \quad V_{n+2} = PV_{n+1} - QV_n.$$

For all *odd* relatively prime values of P and Q such that $P^2 - 4Q$ is positive, Ribenboim and McDaniel [6] recently determined all indices n such that U_n, $2U_n$, V_n or $2V_n$ is a square($= \square$). (See introduction in [6] for known other results.)

In this paper, we consider the above problem when P is even and $Q = -1$. Using elementary properties of elliptic curves as well as the methods in [6], we show that if $P = 2t$ with t even and $Q = -1$, then U_n, $2U_n$, V_n or $2V_n = \square$ implies $n \leq 3$ under some assumptions.

Applying these results, we prove some theorems concerning Diophantine equations of the forms

$$4x^4 - Dy^2 = \pm 1, \quad x^4 - Dy^2 = -1, \quad x^2 - 4Dy^4 = \pm 1, \quad x^2 - Dy^4 = 1.$$

This provides the main result of Kagawa [3], who uses Baker theory, with an elementary proof.

T. Kagawa: Department of Mathematics, School of Science and Engineering, Waseda University, Ohkubo, Shinjuku, Tokyo 169, Japan. e-mail: kagawa@mn.waseda.ac.jp

N. Terai: Division of General Education, Ashikaga Institute of Technology, 268–1 Omae, Ashikaga, Tochigi 326, Japan. e-mail: terai@aitsun5.ashitech.ac.jp

Mathematics Subject Classification (1991): Primary 11B39; Secondary 11D25

2. Preliminaries

Let t be even and $D = t^2 + 1$. The sequences $\{v_n\}$, $\{u_n\}$ are defined by

$$\begin{cases} v_0 = 1, \quad v_1 = t, \quad v_{n+2} = 2tv_{n+1} + v_n, \\ u_0 = 0, \quad u_1 = 1, \quad u_{n+2} = 2tu_{n+1} + u_n. \end{cases} \tag{1}$$

Note that $v_n = V_n/2$ and $u_n = U_n$ for all integers n. We easily find from (1) that

$$v_n \text{ is even} \iff n \text{ is odd}, \qquad u_n \text{ is even} \iff n \text{ is even}.$$

We also have the following relations:

$$v_n^2 - Du_n^2 = (-1)^n, \quad v_{-n} = (-1)^n v_n, \quad u_{-n} = (-1)^{n+1} u_n, \tag{2}$$

$$v_{m+n} = v_m v_n + Du_m u_n, \quad u_{m+n} = v_m u_n + v_n u_m, \tag{3}$$

$$v_{2n} = 2v_n^2 + (-1)^{n+1}, \quad u_{2n} = 2v_n u_n, \tag{4}$$

$$\begin{cases} v_{3n} = v_n\,(4v_n^2 + 3(-1)^{n+1}), \\ u_{3n} = u_n(4v_n^2 + (-1)^{n+1}), \end{cases} \tag{5}$$

$$\begin{cases} v_{5n} = v_n\,\{16v_n^4 + (-1)^{n+1}20v_n^2 + 5\}, \\ u_{5n} = u_n\{16v_n^4 + (-1)^{n+1}12v_n^2 + 1\}, \end{cases} \tag{6}$$

$$\begin{cases} v_{7n} = v_n\,\{64v_n^6 + (-1)^{n+1}112v_n^4 + 56v_n^2 + (-1)^{n+1} \cdot 7\}, \\ u_{7n} = u_n\{64v_n^6 + (-1)^{n+1}80v_n^4 + 24v_n^2 + (-1)^{n+1}\}. \end{cases} \tag{7}$$

It is clear from (1) that if $n > 0$, then $v_n, u_n > 0$. Thus from (2) if $n < 0$, then

$$v_n > 0 \iff n \text{ is even}, \qquad u_n > 0 \iff n \text{ is odd}.$$

We need the following Diophantine lemmas which will be used in the proofs of the theorems.

Lemma 1 (Ljunggren [4]). *The Diophantine equation*

$$x^2 - 3y^4 = 1$$

has only the positive integral solutions $(x, y) = (2, 1), (7, 2)$.

Lemma 2. *The Diophantine equation*

$$x^2 - Dy^4 = 1 \quad (D = 12, 111, 444)$$

has no positive integral solutions x, y.

(See Mordell [5] for the cases $D = 12$, 444, and Cohn [1] for the case $D = 111$.)

3. Theorems

For a prime p and an integer $t \neq 0$, let $e_p(t)$ be the integer such that $p^{e_p(t)}$ exactly divides t. We assume that t is an even integer such that

$$e_p(t) \text{ is odd for } p = 3, 5 \text{ or } 7.$$

In this paper, we devote ourselves to the study of this case.

Under this assumption, we prove the following:

Theorem 1. *The equation* $v_n = 2\square$ *has only the solution* $n = 3$, $t = 6$, $D = 37$.

Theorem 2. *The equation* $v_n = \square$ *with* n *odd has no solutions.*

Theorem 3. *The equation* $u_n = 2\square$ *has only the solution* $n = 0$.

Theorem 4. *The equation* $u_n = \square$ *with* n *even has only the solution* $n = 0$.

Proof of Theorem 1. Since v_n is even, we see that n is odd. Thus if $n < 0$, then $v_n < 0$. Hence we may suppose that $n > 0$.

The proof is divided into two cases: $n \equiv 0 \pmod p$ and $n \not\equiv 0 \pmod p$ with $p = 3, 5$ or 7.

Case 1: $n \equiv 0 \pmod p$. Then let $n = pk$. Note that k is odd.

(i) If $p = 3$, then from (5) we have $v_{3k} = v_k(4v_k^2 + 3) = 2\square$. Since k is odd and $t \equiv 0 \pmod 3$, we see from (1) that $v_k \equiv 0 \pmod 3$, so $\gcd(v_k, 4v_k^2 + 3) = 3$. Thus we have

$$v_k = 2 \cdot 3x_1^2 \text{ and } 4v_k^2 + 3 = 3x_2^2,$$

so

$$3(2x_1)^4 + 1 = x_2^2.$$

It follows from Lemma 1 that $x_1 = 1, x_2 = 7, v_k = 6$. Hence from (2) we obtain $D = 37, t = 6, k = 1, n = 3$.

(ii) If $p = 5$, then from (6) we have $v_{5k} = v_k(16v_k^4 + 20v_k^2 + 5) = 2\square$. Since k is odd and $t \equiv 0 \pmod 5$, we see that $\gcd(v_k, 16v_k^4 + 20v_k^2 + 5)$ is 5. Thus we have

$$v_k = 2 \cdot 5x_1^2 \text{ and } 16v_k^4 + 20v_k^2 + 5 = 5x_2^2,$$

so

$$(2^2 \cdot 5x_1^2)^4 + 5(2^2 \cdot 5x_1^2)^2 + 5 = 5x_2^2.$$

Hence we obtain the elliptic curve

$$E : Y^2 = X^3 + 5^2X^2 + 5^3X$$

with $x_3 = 2^2 \cdot 5x_1^2$, $X = 5x_3^2$, $Y = 5^2 x_3 x_2$. The substitution $X = X' - 8$, $Y = Y'$ yields the elliptic curve

$$E' : Y'^2 = X'^3 + X'^2 - 83X' + 88,$$

which is the curve 400F1 in Cremona's table [2]. Thus we see that the Mordell-Weil group $E'(\mathbf{Q})$ of E' over $\mathbf{Q}$ is given by $E'(\mathbf{Q}) = \langle(8,0)\rangle \cong \mathbf{Z}/2\mathbf{Z}$. Therefore we have $E(\mathbf{Q}) = \{O, (0,0)\}$, $x_1 = 0$, so $v_k = 0$, which contradicts $v_k > 0$.

(iii) If $p = 7$, then we similarly have from (7)

$$v_k = 2 \cdot 7x_1^2 \text{ and } 64v_k^6 + 112v_k^4 + 56v_k^2 + 7 = 7x_2^2,$$

so the elliptic curve

$$E : Y^2 = X^3 + 7^2X^2 + 2 \cdot 7^3X + 7^4$$

with $x_3 = (2^2 \cdot 7x_1^2)^2$, $X = 7x_3$, $Y = 7^2x_2$. The substitution $X = X' - 16$, $Y = Y'$ yields

$$E' : Y'^2 = X'^3 + X'^2 - 114X' - 127,$$

which is the curve 196B1 in Cremona's table [2]. Thus we see that $E'(\mathbf{Q}) = \langle(16,49)\rangle \cong \mathbf{Z}/3\mathbf{Z}$. We therefore have $E(\mathbf{Q}) = \{O, (0, \pm 49)\}$, $x_3 = 0$, $x_1 = 0$, so $v_k = 0$, which contradicts $v_k > 0$.

Case 2: $n \not\equiv 0 \pmod p$. Then we can put $n = pk \pm l$, where k is even and l is odd with $1 \le l < p$.

Now suppose that $d = e_p(t)$ is odd. From (2) and (3), we have $v_{pk\pm l} = \pm v_{pk}v_l + Du_{pk}u_l = 2\square$. Then the following claim holds:

Claim. (a) $e_p(v_l) = d$, $e_p(u_l) = 0$. (b) $e_p(v_{pk}) = 0$, $e_p(u_{pk}) \ge d + 1$.

The claim above implies that $e_p(v_{pk\pm l}) = d$, which is impossible, since d is odd and $v_{pk\pm l} = 2\square$. Thus to prove Theorem 1, it suffices to show the claim.

Proof of claim. (a) Since l is odd ($< p \le 7$), we have $l = 1, 3, 5$. Then $v_1 = t$, $v_3 = t(4t^2+3)$, $v_5 = t(16t^4 + 20t^2 + 5)$. These imply that $e_p(v_l) = d$ for each l, p with $1 \le l < p \le 7$. From $(v_l, u_l) = 1$, we have $e_p(u_l) = 0$.

(b) Since k is even, we have $u_k \equiv 0 \pmod t$, so $e_p(u_k) \ge d$, $e_p(v_k) = 0$. Since $v_{pk} + u_{pk}\sqrt{D} = (v_k + u_k\sqrt{D})^p$, we have

$$u_{pk} = u_k \sum_{j=0}^{(p-1)/2} \binom{p}{2j} v_k^{2j} (u_k^2 D)^{\frac{p-1}{2} - j} := u_k \sum_{j=0}^{(p-1)/2} a_j.$$

Then $e_p(u_{pk}) \geq d+1$. In fact, if $j < (p-1)/2$, then $e_p(a_j) \geq d(p-1-2j) > 1$. If $j = (p-1)/2$, then $e_p(a_j) = 1$. Thus $e_p(\sum_{j=0}^{(p-1)/2} a_j) = 1$. From $(v_{pk}, u_{pk}) = 1$, we have $e_p(v_{pk}) = 0$. This completes the proof of the claim and hence of Theorem 1. □

Proof of Theorem 2. Suppose that n is odd.

Case 1: $n \equiv 0 \pmod p$. In the same way as in the proof of Theorem 1, we obtain the following, respectively.

(i) If $p = 3$, then we have the equation

$$12x_1^4 + 1 = x_2^2,$$

which has no non-trivial solutions by Lemma 2.

(ii) If $p = 5$, then we have the elliptic curve defined by

$$Y^2 = X^3 + 5^2X^2 + 5^3X,$$

which implies $X = 0$, so $v_k = 0$, as above.

(iii) If $p = 7$, then we have the elliptic curve defined by

$$Y^2 = X^3 + 7^2X^2 + 2\cdot 7^3X + 7^4,$$

which implies $X = 0$, so $v_k = 0$, as above.

Case 2: $n \not\equiv 0 \pmod p$. Similarly, comparing p-adic values of both sides of $v_n = \square$ leads to a contradiction. □

Remark 1. In the proof of Theorems 1, 2, the fact that the elliptic curves above have rank 0 is a lucky thing. Thus the integral points are very easy to find. When an elliptic curve has positive rank, methods are known for determining the integral points on such a curve, but these methods are far from elementary.

In order to prove Theorems 3, 4, we need the following two propositions:

Proposition 1. *If the equation $u_n = \square$ or $2\square$ with n even > 0 has any solutions, then we have $D = 37$, $n = 2^e \cdot 3$ with $e \geq 1$.*

Proof. Let $n = 2^es$, where $e \geq 1$ and s is odd. Then applying (4) e times yields

$$u_n = 2v_{n/2}u_{n/2} = 2^2v_{n/2}v_{n/4}u_{n/4} = \cdots = 2^e\left(\prod_{j=1}^{e} v_{n/2^j}\right)u_s.$$

Since $v_{n/2^j}$ $(1 \leq j \leq e)$, u_s are pairwise relatively prime, we have $v_s = \square$ or $2\square$ with s odd. By Theorem 2 the first equation has no solutions. By Theorem 1 the second equation has only the solution $s = 3$, $t = 6$, $D = 37$, $n = 2^e \cdot 3$ with $e \geq 1$. □

Proposition 2. *Let $D = 37$ and $n = 2^e \cdot 3$ with $e \geq 1$. Then neither $u_n = \Box$ nor $u_n = 2\Box$ has solutions.*

Proof. Write $n = 3k$, where $k = 2^e$. Then by (2) and (5), we have $u_{3k} = u_k(4 \cdot 37u_k^2 + 3)$. Note that k is even. We see that $u_k \equiv 0 \pmod 3$. Otherwise, $u_n = \Box$ or $2\Box$ implies $4 \cdot 37u_k^2 + 3 = \Box$, which is found impossible by taking modulo 4. Hence it follows from $u_n = \Box$ that

$$u_k = 3x_1^2, \quad 4 \cdot 37u_k^2 + 3 = 3x_2^2,$$

so

$$444x_1^4 + 1 = x_2^2,$$

which has no non-trivial solution by Lemma 2. It also follows from $u_n = 2\Box$ that

$$u_k = 3 \cdot 2 \cdot x_1^2, \quad 4 \cdot 37u_k^2 + 3 = 3x_2^2,$$

so

$$111(2x_1)^4 + 1 = x_2^2,$$

which has no non-trivial solutions by Lemma 2. □

Proof of Theorem 3. Since u_n is even, we see that n is even and hence $n \geq 0$. Thus by (4), we have

$$v_{n/2} = \Box, \quad u_{n/2} = \Box.$$

If $n/2$ is odd, then the first equation has no solution by Theorem 2. If $n/2$ is even, then the second equation has only the solution $n = 0$ by Propositions 1, 2. □

Proof of Theorem 4. Theorem 4 is clear from Propositions 1, 2. □

4. Applications

As a corollary to Theorems in § 3, we now deduce some results concerning the following Diophantine equations. We consider only *non-negative* integral solutions.

Now suppose that $X = a$, $Y = b$ is the fundamental solution of the Pell equation $X^2 - DY^2 = -1$. Then the general solution is given by

$$X + Y\sqrt{D} = (a + b\sqrt{D})^n.$$

Let $\alpha = a + b\sqrt{D}$, $\beta = a - b\sqrt{D}$. Then $\alpha + \beta = 2a$, $\alpha\beta = -1$. We now define for all integers n

$$v_n = \frac{1}{2}(\alpha^n + \beta^n), \quad u_n = \frac{1}{2\sqrt{D}}(\alpha^n - \beta^n).$$

Then we have $v_{n+2} = 2av_{n+1} + v_n$ and $u_{n+2} = 2au_{n+1} + u_n$.

Now let $a = t$ and $D = t^2 + 1$. Then $X = t$, $Y = 1$ is the fundamental solution of the Pell equation $X^2 - DY^2 = -1$. As in § 3, we assume that t is an even integer such that $e_p(t)$ is odd for $p = 3, 5$ or 7.

Theorem 1′. *The equation*

$$4x^4 - Dy^2 = \pm 1$$

has only the solution $x = 21$, $y = 145$, $D = 37$.

For, $2x^2 = v_n$, and hence by Theorem 1 we have $n = 3$, $D = 37$.

Hence this provides an elementary proof of the main result in Kagawa [3]. Note that the curve $4x^4 - 37y^2 = -1$ is birationally equivalent over $\mathbf{Q}$ to the elliptic curve $y^2 = x^3 - 37^2x$, whose rank is 1.

Theorem 2′. *The equation*

$$x^4 - Dy^2 = -1$$

has no solutions.

For, $x^2 = v_n$ with n odd, and hence by Theorem 2 we have no solutions.

Theorem 3′. *The equation*

$$x^2 - 4Dy^4 = \pm 1$$

has only the solution $x = 1$, $y = 0$.

For, $2y^2 = u_n$, and hence by Theorem 3 we have $x = 1$, $y = 0$.

Theorem 4′. *The equation*

$$x^2 - Dy^4 = 1$$

has only the solution $x = 1$, $y = 0$.

For, $y^2 = u_n$ with n even, and hence by Theorem 4 we have $x = 1$, $y = 0$.

References

[1] Cohn, J.H.E.: The Diophantine equation $y^2 = Dx^4 + 1$, III. Math. Scand. **42**, 180–188 (1978)
[2] Cremona, J.E.: *Algorithms for modular elliptic curves*. Second edition, Cambridge Univ. Press, 1997
[3] Kagawa, T.: The Diophantine equation $4x^4 - 37y^2 = -1$. Preprint
[4] Ljunggren, W.: Einige Eigenschaften der Einheiten reeller quadratischer und reinbiquadratischer Zahlkörper. Oslo Vid.-Akad. Skrifter **1** (1936), Nr. 12
[5] Mordell, L.J.: The Diophantine equation $y^2 = Dx^4 + 1$. J. London Math. Soc. **39**, 161–164 (1964)
[6] Ribenboim, P. and McDaniel, W.L.: The square terms in Lucas sequences. J. Number Theory **58**, 104–123 (1996)