*Acta Academiae Paedagogicae Agriensis, Sectio Mathematicae* **30** *(2003) 75–86*

# REPRESENTATION OF SOLUTIONS OF PELL EQUATIONS USING LUCAS SEQUENCES

**James P. Jones (Calgary, Canada)**

*Dedicated to the memory of Professor Péter Kiss*

**Abstract.** We consider classes of Pell equations of the form $x^2-dy^2=c$ where $d=a^2\pm4$ or $d=a^2\pm1$ and $c=\pm4$ or $c=\pm1$. We show that all the solutions are expressible in terms of Lucas sequences and we give the Lucas sequences which solve the equations explicitly.

**AMS Classification Number:** 11B39, 11B37

## 1. Introduction

The purpose of this paper is to collect together results concerning the solutions of the Pell equations $x^2-(a^2\pm4)y^2=\pm4$, $x^2-(a^2\pm4)y^2=\pm1$, $x^2-(a^2\pm1)y^2=\pm4$ and $x^2-(a^2\pm1)y^2=\pm1$. We show that the solutions to these Pell equations can all be expressed in terms of Lucas sequences $U_n(a,\pm1)$ and $V_n(a,\pm1)$ of E. Lucas [20], [21].

The solutions of the Pell equations $x^2-(a^2+4)y^2=\pm a$, $x^2-(a^2-4)y^2=5-2a$, $x^2-(a^2-4)y^2=2-a$ and $x^2-(a^2-1)y^2=2-2a$ can also be represented as Lucas sequences. This is more difficult to prove however and will be shown in a subsequent paper.

The above Pell equations are important to logicians since the sequences of solutions have many elegant divisibility properties which make them useful for diophantine representation of recursively enumerable sets. The above mentioned Pell equations can be found in the papers Y. Matiyasevich [22], [25], M. Davis [1], J. Robinson [26], [27], [28], M. Davis, H. Putnam, J. Robinson [3] and Davis, Matiyasevich and Robinson [2]. Also in the author's papers [4], [5], [6], [7], and in Jones and Matiyasevich [8], [10]. The above Pell equations also have application to the problem of singlefold diophantine representation of recursively enumerable sets. See Matiyasevich [25] for an explanation, also the paper of Sun Zhiwei [29] and Jones and Matiyasevich [8], [9].

Let $A$ and $B$ be integers with $A\geq1$ and $B=\pm1$. Put $D=A^2-4B$. The Pell equation,

$$V^2-DU^2=\pm4, \tag{1}$$

is closely connected with the Lucas identity,

$$V_n^2 - DU_n^2 = 4B^n \tag{2}$$

which is satisfied by the Lucas sequences $U_n$ and $V_n$. In the theory developed by E. Lucas [20], [21] and D. H. Lehmer [18], [19], the sequences $U_n = U_n(A, B)$ and $V_n = V_n(A, B)$ satisfying equation (2) are definable as second order linear recurrences:

$$V_0 = 2,\ V_1 = A,\ V_{n+2} = AV_{n+1} - BV_n, \tag{3}$$

$$U_0 = 0,\ U_1 = 1,\ U_{n+2} = AU_{n+1} - BU_n. \tag{4}$$

The Lucas sequences $V_n$ and $U_n$ satisfy a large number of other identities as well. We shall need:

$$(i)\ \ 2V_{n+1} = AV_n + DU_n, \qquad (ii)\ \ 2U_{n+1} = AU_n + V_n, \tag{5}$$

$$(i)\ \ 2BV_{n-1} = AV_n - DU_n, \qquad (ii)\ \ 2BU_{n-1} = AU_n - V_n. \tag{6}$$

The above four identities are easy to derive, by induction on $n$, from the recurrence equations (3) and (4). Using identity (5) (i) it is then easy to show that $U_n$ and $V_n$ satisfy the Lucas identity (2). For plainly $V_n^2 - DU_n^2 = 4B^n$ holds for $n = 0$. Suppose it holds for $n$. By (5) (i),

$$4V_{n+1}^2 - 4DU_{n+1}^2 = (AV_n + DU_n)^2 - D(AU_n + V_n)^2$$

$$= A^2V_n^2 + D^2U_n^2 - DA^2U_n^2 - DV_n^2 = (A^2 - D)V_n^2 - (A^2 - D)DU_n^2$$

$$= 4BV_n^2 - 4BDU_n^2 = 4B(V_n^2 - DU_n^2) = 4B4B^n = 16B^{n+1}.$$

Hence the Lucas identity (2) holds for $n + 1$ and so by induction (2) holds for all $n \geq 0$.

One of the main theorems we shall need is that all solutions of $V^2 - DU^2 = \pm 4$ are given by the Lucas sequences $V = V_n(A, B)$ and $U = U_n(A, B)$. And we shall need to know exactly for which pairs $(A, B)$ this holds. We therefore give a careful proof and an exact statement. We will prove the theorem in the following form:

**Theorem 1.1.** *Suppose $D = A^2 - 4B$, $B = 1$ and $3B + 5 \leq 2A$. Then for all nonnegative integers $U$ and $V$,*

$$V^2 - DU^2 = \pm 4 \iff (\exists n \geq 0)[V = V_n(A, B) \ \ \textit{and} \ \ U = U_n(A, B)]$$

Before giving the proof we mention that the purpose of the hypothesis $3B+5 \leq 2A$ is to exclude some pairs such as $B = 1$ and $A = 3$ for which the theorem does not hold, yet include others such as $B = -1$ and $A = 1$ for which it does hold. If $B = 1$ and $A = 3$, then $D = 5$. $x^2 - 5y^2 = -4$ has infinitely many nonnegative integer solutions $(x, y)$. But they are not all of the form $x = V_n(3, 1)$ and $y = U_n(3, 1)$. For example the solution $(x, y) = (1, 1)$ is not of the form $x = V_n(3, 1)$ and $y = U_n(3, 1)$. Rather $x = V_n(1, -1)$ and $y = U_n(1, -1)$ where $n = 1$. $(x, y)$ lies within the Fibonacci sequence.

Care is therefore necessary in the statement of Theorem 1.1. Not only can Theorem 1.1 fail to hold when $B = 1$ and $A = 3$, the result can fail to hold when we try to generalize it beyond $|B| = 1$. Consider for example the case of $B = 2$. If $A = 4$, then $D = A^2 - 4B = 8$. Now $V = 20$ and $U = 7$ is a solution of $V^2 - 8U^2 = 4B^1$. But $\forall n\ 20 \neq V_n(4, 2)$ and $\forall n\ 7 \neq U_n(4, 2)$. Thus Theorem 1.1 does not hold for $B = 2$ and $A = 4$.

## 2. Descent

Our main tool in the proof we shall give here of Theorem 1.1 will be Fermat's method of descent. We will apply the method to equation (1). We will need the following lemmas:

**Lemma 2.1.** (Parity Lemma) *Suppose $A$ is a positive integer and $|B| = 1$.*
*If $A$ is even: $V_n(A, B)$ is even, and $U_n(A, B)$ is even iff $2|n$.*
*If $A$ is odd: $V_n(A, B) \equiv U_n(A, B) \pmod 2$, and $V_n(A, B)$ and $U_n(A, B)$ are even iff $3|n$.*

**Proof.** By induction on $n$ using equations (3) and (4).

**Lemma 2.2.** *For all $n \geq 0$, $V_{2n}(1, -1) = V_n(3, +1)$ and $U_{2n}(1, -1) = U_n(3, +1)$, $(n = 0, 1, 2, \ldots)$.*

**Proof.** The proof of this for $V_n$ is the same as that for $U_n$ so we shall give only the proof for $U_n$. For this we use induction on $n$. If $n = 0$ or $n = 1$, then $U_{2n}(1, -1) = U_n(3, 1)$ and $U_{2(n+1)}(1, -1) = U_{n+1}(3, 1)$. Suppose these hold for $n$ and $n+1$. By (4), $U_{2(n+2)}(1, -1) = U_{2n+4}(1, -1) = U_{2n+3}(1, -1) + U_{2n+2}(1, -1) =$
$U_{2n+2}(1, -1) + U_{2n+1}(1, -1) + U_{2n+2}(1, -1) =$
$U_{2n+2}(1, -1) + U_{2n+2}(1, -1) - U_{2n}(1, -1) + U_{2n+2}(1, -1) =$
$3U_{2n+2}(1, -1) - U_{2n}(1, -1) = 3U_{2(n+1)}(1, -1) - U_{2n}(1, -1) =$
$3U_{n+1}(3, 1) - U_n(3, 1) = U_{n+2}(3, 1)$.

**Lemma 2.3.** *Let $A$ and $V$ be non-negative integers. Then*
*If $V^2 - A^2 = +8$, then $A = 1$ and $V = 3$.*

*If* $V^2 - A^2 = -8$, *then* $A = 3$ *and* $V = 1$.

**Proof.** $1 \le |V^2 - A^2| \le 8 \Rightarrow 1 \le |V - A|(V + A) \le 8 \Rightarrow 1 \le V + A \le 8$. Hence, if $V^2 - A^2 = +8$, then $A = 1$ and $V = 3$. If $V^2 - A^2 = -8$, then $A = 3$ and $V = 1$.

**Lemma 2.4.**

(Descent Lemma) Suppose $D = A^2 - 4B$, $B = \pm 1$, $B + 2 \le A$ and $U$ and $V$ are integers such that $0 \le V$, $2 \le U$ and $V^2 - DU^2 = \pm 4$. If $V'$ and $U'$ are defined by

$$(7) \qquad (i)\;\; V' = \frac{AV - DU}{2B}, \qquad (ii)\;\; U' = \frac{AU - V}{2B},$$

then $V'$ and $U'$ are integers and satisfy $V'^2 - DU'^2 = \pm 4B$. Also $V'$ and $U'$ satisfy

$$(8) \qquad (i)\;\; 2V = AV' + DU, \qquad (ii)\;\; 2U = AU' + V'.$$

Furthermore $1 \le V'$ and $1 \le U' < U$.

**Proof.** First we show that $2U \le V$. Since $D = A^2 - 4B$, $B = \pm 1$ and $B + 2 \le A$, $5 \le D$. Since $2 \le U$ we have $4 \le U^2$ and so $4U^2 \le 5U^2 \pm 4 \le DU^2 \pm 4 = V^2$. Therefore $2U \le V$.

Next we show that $V'$ and $U'$ are integers. $D = A^2 - 4B \Rightarrow D \equiv A^2 \equiv A \pmod 2$. Also $V^2 - DU^2 = \pm 4 \Rightarrow V^2 \equiv A^2U^2 \pmod 2 \Rightarrow V \equiv AU \pmod 2$. Hence $AU - V \equiv 0 \pmod 2$ and so $U'$ is an integer. Also since $V \equiv AU \pmod 2$ and $D \equiv A \pmod 2$, $AV - DU \equiv A^2U - AU \equiv AU - AU = 0 \pmod 2$ so $V'$ is an integer.

Next we show that $(V')^2 - D(U')^2 = \pm 4B$. From the definitions of $V'$ and $U'$ we have

$$V'^2 - DU'^2 = \frac{(AV - DU)^2}{4B^2} - D\frac{(AU - V)^2}{4B^2} =$$

$$\frac{A^2V^2 - DV^2 - DA^2U^2 + D^2U^2}{4B^2} =$$

$$\frac{(A^2 - D)(V^2 - DU^2)}{4B^2} = \frac{(4B)(\pm 4)}{4B^2} = \frac{\pm 4}{B} = \pm 4B.$$

Next we show that $2V = AV' + DU'$ and $2U = AU' + V'$. From the definitions of $V'$ and $U'$,

$$AV' + DU' = A\frac{AV - DU}{2B} + D\frac{AU - V}{2B} = \frac{A^2V - DV}{2B} = \frac{V(A^2 - D)}{2B} = \frac{V4B}{2B} = 2V.$$

Also

$$AU' + V' = A\frac{AU - V}{2B} + \frac{AV - DU}{2B} = \frac{A^2U - DU}{2B} = \frac{U(A^2 - D)}{2B} = \frac{U4B}{2B} = 2U.$$

Next we show that $1 \le U' < U$. $V^2 - DU^2 = \pm 4 \Rightarrow (A^2 - 4B)U^2 - V^2 = \mp 4 \Rightarrow A^2U^2 - V^2 = 4BU^2 \mp 4 \Rightarrow (AU - V)(AU + V) = 4B(U^2 \mp B)$. Since $2BU' = AU - V \Rightarrow 2BU'(AU + V) = 4B(U^2 \mp B) \Rightarrow U'(AU + V) = 2(U^2 \mp B) = 2U^2 \mp 2B$, we have

$$\text{(9)} \qquad \frac{2U^2 - 2}{AU + V} \le U' = \frac{2U^2 \mp 2B}{AU + V} \le \frac{2U^2 + 2}{AU + V} \le \frac{2U^2 + 2}{U + V},$$

using $B + 2 \le A \Rightarrow 1 \le A$. Since $2 \le U \Rightarrow 2 < 2U^2 \Rightarrow 0 < 2U^2 - 2$, equation (9) $\Rightarrow 0 < U'$. Hence $1 \le U'$. Now we can show $U' < U$. Using $2U \le V$, shown earlier, $2U \le V \Rightarrow 3U \le U + V$. Also $2 \le U \Rightarrow 2 < U^2$. Hence by (9),

$$\text{(10)} \qquad U' \le \frac{2(U^2 + 2)}{U + V} \le \frac{2U^2 + 2}{3U} \le \frac{2U^2 + U^2}{3U} = U.$$

Therefore $U' < U$. Finally we can show that $1 \le V'$. Since $V' = (AV - DU)/2B$, we have

$$\text{(11)} \quad UV' = \frac{AUV - DU^2}{2B} = \frac{AUV - V^2 \pm 4}{2B} = \frac{AUV - V^2}{2B} \pm 2B = VU' \pm 2B.$$

Since $1 \le U'$ and $4 \le 2U \le V$, we have $2 \le 4 \pm 2B \le 2U \pm 2B \le 2UU' \pm 2B \le VU' \pm 2B = UV'$ by (11). Hence $2 \le UV'$ and so $1 \le V'$. This completes the proof of the Descent Lemma.

**Proof of Theorem 1.1.** Suppose $3B + 5 \le 2A$. In the direction $\Leftarrow$ Theorem 1.1 has already been proven by our establishing identity (2). For the direction $\Rightarrow$ we use the Descent Lemma and induction on $U$. Suppose $0 \le U$, $0 \le V$ and $V^2 - DU^2 = \pm 4$. If $U = 0$, then $V^2 = \pm 4 \Rightarrow V^2 = 4 \Rightarrow V = 2$ and so we can let $n = 0$. Suppose $U = 1$. Then $V^2 - DU^2 = \pm 4 \Rightarrow V^2 - (A^2 - 4B) = \pm 4 \Rightarrow V^2 - A^2 = \pm 4 - 4B$. We consider two cases:

**Case 1.** $B = -1$. Here we have $V^2 - A^2 = 0$ or $V^2 - A^2 = 8$. If $V^2 - A^2 = 0$, then $V = A$ and so we can let $n = 1$ since $V_1(A, B) = A = V$ and $U_1(A, B) = 1 = U$. If $V^2 - A^2 = 8$, then by Lemma 2.3, $A = 1$ and $V = 3$ so we can let $n = 2$ since $V_2(A, B) = A^2 - 2B = 3 = V$ and $U_2(A, B) = A = 1 = U$.

**Case 2.** $B = +1$. Here $V^2 - A^2 = 0$ or $V^2 - A^2 = -8$. If $V^2 - A^2 = -8$, then by Lemma 2. 3, $A = 3$ and $V = 1$. Since $B = 1$, $A = 3$ contradicts $3B + 5 \le 2A$. Hence $V^2 - A^2 = 0$. In this case $V = A$ and so we can let $n = 1$ since $V_1(A, B) = A = V$ and $U_1 = 1 = U$.

Now we can suppose $2 \le U$ and that the implication $\Rightarrow$ of Theorem 1. 1 holds for all pairs $V'$, $U'$ such that $0 \le U' < U$ and $0 \le V'$. Since $B = \pm 1$, the hypothesis $3B + 5 \le 2A$ implies $B + 2 \le A$ and so we can apply the Descent lemma. Define $V'$ and $U'$ from $V$ and $U$ as indicated in the Descent Lemma: $V' = (AV - DU)/2B$ and $U' = (AU - V)/2B$. The Descent Lemma then asserts that $V'$ and $U'$ are integers, $1 \le V'$, $1 \le U' < U$ and $V'^2 - DU'^2 = \pm 4$. Hence by the induction hypothesis $\exists n \ge 0$ such that $V' = V_n(A, B)$ and $U' = U_n(A, B)$. Consequently using equations (8) in the Descent Lemma and identity (5) (i) we have, $2V = AV' + DU' = AV_n + DU_n = 2V_{n+1}$ and so $V = V_{n+1}$. By (8) and identity (5) (ii) we also have $2U = AU' + V' = AU_n + V_n = 2U_{n+1}$ and so $U = U_{n+1}$. Thus the implication $\Rightarrow$ holds for $U$. By induction the implication $\Rightarrow$ holds for all $U$. Thus Theorem 1. 1 is proved.

**Corollary 2.5.** *If $4 \le A$, $B = 1$, $D = A^2 - 4$, then $V^2 - DU^2 = -4$ has no solutions $U$, $V$.*

**Proof.** Of course this follows immediately from Theorem 1. 1 and Lucas Identity (2). But there is a more interesting proof using the Descent Lemma: Suppose $4 \le A$, $B = +1$ and $D = A^2 - 4$. Then $B + 2 \le A$ so we can use the Descent Lemma. Suppose $V^2 - DU^2 = -4$ for some $V$, $U$. Let $(V, U)$ be the pair with smallest $U$ such that $0 \le V$ and $0 \le U$. Then $U \ne 0$. By Lemma 2. 3, $U = 1$ would imply $A = 3$. Hence $2 \le U$ and so by the Descent Lemma $\exists V'$, $U'$ such that $1 \le V'$, $1 \le U' < U$ and $V^2 - DU^2 = -4$. But this contradicts the original choice of $U$ and $V$. Thus $V$ and $U$ such that $V^2 - DU^2 = -4$ do not exist.

**Remark.** If $A = 3$, then $V^2 - (A^2 - 4)U^2 = -4$ does have solutions, e.g. $V = 1$ and $U = 1$.

**Corollary 2.6.** *If $4 \le A$, then $x^2 - (a^2 - 4)y^2 = -4$ has no solutions.*

**Corollary 2.7.** *If $4 \le A$, then all solutions of $x^2 - (a^2 - 4)y^2 = +4$ are given by $x = V_i(a, +1)$ and $y = U_i(a, +1)$, $(i = 0, 1, 2, \ldots)$.*

**Corollary 2.8.** *If $1 \le A$, then all solutions of $x^2 - (a^2 + 4)y^2 = -4$ are given by $x = V_{2i+1}(a, -1)$ and $y = U_{2i+1}(a, -1)$, $(i = 0, 1, 2, \ldots)$.*

**Corollary 2.9.** (Matiyasevich equation [22]) *If $1 \le A$, then all solutions of $x^2 - (a^2 + 4)y^2 = +4$ are given by $x = V_{2i}(a, -1)$ and $y = U_{2i}(a, -1)$, $(i = 0, 1, 2, \ldots)$.*

**Remark.** In [22] Y. V. Matiyasevich used the above equation $x^2 - (a^2 + 4)y^2 = 4$ with $a = 1$, to solve Hilbert's Tenth Problem. (I.e. he used the sequence of Fibonacci numbers with even subscripts, $U_{2i}(1, -1) = U_i(3, 1)$.)

## 3. Solutions of Pell equations with $d = a^2 \pm 4$ and $c = \pm 1$.

In this section we give the solutions of Pell equations of the form $x^2 - (a^2 \pm 4)y^2 = \pm 1$.

**Lemma 3.1.** *If $4 \le a$, then $x^2 - (a^2 - 4)y^2 = -1$ has no solutions.*

**Proof.** Suppose $4 \le a$ and $x^2 - (a^2 - 4)y^2 = -1$. Multiplying by 4 we obtain $(2x)^2 - (a^2 - 4)(2y)^2 = -4$, which, since $4 \le a$, has no solutions by Corollary 2.6.

**Remark.** If $a = 3$, then $x^2 - (a^2 - 4)y^2 = -1$ has infinitely many solutions, $x = V_{6i+3}(1,-1)/2$ and $y = U_{6i+3}(1,-1)/2$, $(i = 0, 1, 2, \ldots)$. This is shown by the next theorem since $a^2 - 4 = 5 = 1^2 + 4$.

**Theorem 3.2.** *If $1 \le a$ and $a$ is odd, then all solutions of $x^2 - (a^2 + 4)y^2 = -1$ are given by $x = \frac{V_{6i+3}(a,-1)}{2}$ and $y = \frac{U_{6i+3}(a,-1)}{2}$, $(i = 0, 1, 2, \ldots)$.*

**Proof.** Using Corollary 2.8, since $1 \le a$, we have $x^2 - (a^2 + 4)y^2 = -1 \iff (2x)^2 - (a^2 + 4)(2y)^2 = -4 \iff 2x = V_n(a, -1)$ and $2y = U_n(a, -1)$ for some odd $n$. As $a$ is odd, by the Parity Lemma $2|V_n(a, -1)$ and $2|U_n(a, -1) \iff 3|n$. $3|n$ and $n$ is odd $\iff \exists i\ n = 6i + 3$, $(i = 0, 1, 2, \ldots)$.

**Lemma 3.3.** *For any even integer $a$, $x^2 - (a^2 + 4)y^2 = -1$ has no solutions.*

**Proof.** Suppose $a$ is even. Then $4|a^2 \Rightarrow 4|a^2 - 4$. But $x^2 \ne -1 \pmod 4$.

**Theorem 3.4.** *If $4 \le a$ and $a$ is even, then all solutions of $x^2 - (a^2 - 4)y^2 = +1$ are given by $x = \frac{V_{2i}(a,+1)}{2}$ and $y = \frac{U_{2i}(a,+1)}{2}$, $(i = 0, 1, 2, \ldots)$.*

**Proof.** Using Corollary 2.7, since $4 \le a$, we have $x^2 - (a^2 - 4)y^2 = +1 \iff (2x)^2 - (a^2 - 4)(2y)^2 = +4 \iff \exists\ n \ge 0$, $2x = V_n(a, +1)$ and $2y = U_n(a, +1)$. Since $2|a$, the Parity Lemma implies $2|V_n(a, +1)$ and $2|U_n(a, +1) \iff 2|n$, i.e. $n = 2i$, $(i = 0, 1, 2, \ldots)$.

**Theorem 3.5.** *If $3 \le a$ and $a$ is odd, then all solutions of $x^2 - (a^2 - 4)y^2 = +1$ are given by $x = \frac{V_{3i}(a,+1)}{2}$ and $y = \frac{U_{3i}(a,+1)}{2}$, $(i = 0, 1, 2, \ldots)$.*

**Proof.** Suppose $3 \le a$ and $a$ is odd. $x^2 - (a^2 - 4)y^2 = +1 \iff (2x)^2 - (a^2 - 4)(2y)^2 = +4$. If $3 < a$, then by Corollary 2.7, $2x = V_n(a, +1)$ and $2y = U_n(a, +1)$, where, by the Parity Lemma, $n = 3i$, $(i = 0, 1, 2, \ldots)$. If $3 = a$, then, since $a^2 - 4 = 5 = 1^2 + 4$, Corollary 2.9, $\Rightarrow 2x = V_{2j}(1, -1)$ and $2y = U_{2j}(1, -1)$, where $j = 3i$, $(i = 0, 1, 2, \ldots)$ by the Parity Lemma, so that $x = V_{6i}(1, -1)/2$ and $y = U_{6i}(1, -1)/2$, $(i = 0, 1, 2, \ldots)$. However by Lemma 2.2, $V_{6i}(1, -1) = V_{3i}(3, +1)$ and $U_{6i}(1, -1) = U_{3i}(3, +1)$, $(i = 0, 1, 2, \ldots)$ as required

**Theorem 3.6.** *If $2 \le a$ and $a$ is even, then all solutions of $x^2 - (a^2 + 4)y^2 = +1$ are given by $x = \frac{V_{2i}(a,-1)}{2}$ and $y = \frac{U_{2i}(a,-1)}{2}$, $(i = 0, 1, 2, \ldots)$.*

**Proof.** By Corollary 2.9, since $1 \le a$, we have $x^2 - (a^2 + 4)y^2 = +1 \iff (2x)^2 - (a^2 + 4)(2y)^2 = +4 \iff 2x = V_n(a, -1)$ and $2y = U_n(a, -1)$ for some even $n$. Since $2|a$ and $n$ is even, the Parity Lemma implies $2|V_n(a, -1)$ and $2|U_n(a, -1)$.

**Theorem 3.7.** *If $1 \le a$ and $a$ is odd, then all solutions of $x^2 - (a^2 + 4)y^2 = +1$ are given by $x = \frac{V_{6i}(a,-1)}{2}$ and $y = \frac{U_{6i}(a,-1)}{2}$, $(i = 0, 1, 2, \ldots)$.*

**Proof.** By Corollary 2.9, since $1 \le a$, we have $x^2 - (a^2 + 4)y^2 = +1 \iff (2x)^2 - (a^2 + 4)(2y)^2 = +4 \iff 2x = V_n(a, -1)$ and $2y = U_n(a, -1)$ for some even $n$. Since

$a$ is odd, the Parity Lemma implies $2|V_n(a,-1)$ and $2|U_n(a,-1) \iff 3|n$. $2|n$ and $3|n \iff 6|n$. Hence $n = 6i$ $(i = 0, 1, 2, \ldots)$.

## 4. Solutions of Pell equations with $d = a^2 \pm 1$ and $c = \pm 1$.

In this section we consider solutions of Pell equations of the form $x^2 - (a^2 \pm 1)y^2 = \pm 1$.

**Lemma 4.1.** *If $2 \le a$, then $x^2 - (a^2 - 1)y^2 = -1$ has no solutions.*

**Proof.** Suppose $2 \le a$ and $x^2 - (a^2 - 1)y^2 = -1$. Multiplying by 4 we obtain $(2x)^2 - ((2a)^2 - 4)y^2 = -4$. Since $4 \le 2a$, this equation has no solutions by Corollary 2. 6.

[Another proof is also possible. Let $d = a^2 - 1$. The continued fraction expansion of $\sqrt{d}$ is $\sqrt{d} = [a-1;\ \overline{1,\ 2a-2}]$ with period length 2 (even). Hence $x^2 - dy^2 = -1$ is unsolvable.]

**Theorem 4.2.** (Julia Robinson's equation [26], [27]) *If $2 \le a$, then all solutions of $x^2 - (a^2-1)y^2 = +1$ are given by $x = \frac{V_i(2a,+1)}{2}$ and $y = U_i(2a,+1)$, $(i = 0, 1, 2, \ldots)$.*

**Proof.** Suppose $2 \le a$. Using Corollary 2.7, since $4 \le 2a$ we have $x^2 - (a^2 - 1)y^2 = +1 \iff (2x)^2 - ((2a)^2 - 4)y^2 = +4 \iff \exists\ n \ge 0$, $2x = V_n(2a,+1)$ and $y = U_n(2a,+1)$. Since $2a$ is even, the Parity Lemma implies $V_n(2a,+1)$ is even. Hence $2|V_n(2a,+1)$.

**Theorem 4.3.** *If $1 \le a$, then all solutions of $x^2 - (a^2 + 1)y^2 = +1$ are given by $x = \frac{V_{2i}(2a,-1)}{2}$ and $y = U_{2i}(2a,-1)$, $(i = 0, 1, 2, \ldots)$.*

**Proof.** Using Corollary 2.9, since $1 \le 2a$, we have $x^2 - (a^2 + 1)y^2 = +1 \iff (2x)^2 - ((2a)^2 + 4)y^2 = +4 \iff 2x = V_n(2a,-1)$ and $y = U_n(2a,-1)$ for some even $n$, $n = 2i$, $(i = 0, 1, 2, \ldots)$. Since $2a$ is even, the Parity Lemma implies $2|V_n(2a,-1)$.

**Theorem 4.4.** *If $1 \le a$, then all solutions of $x^2 - (a^2 + 1)y^2 = -1$ are given by $x = \frac{V_{2i+1}(2a,-1)}{2}$ and $y = U_{2i+1}(2a,-1)$, $(i = 0, 1, 2, \ldots)$.*

**Proof.** Using Corollary 2.8, since $1 \le 2a$, we have $x^2 - (a^2 + 1)y^2 = -1 \iff (2x)^2 - ((2a)^2 + 4)y^2 = -4 \iff 2x = V_n(2a,-1)$ and $y = U_n(2a,-1)$ for some odd $n$, $n = 2i + 1$, $(i = 0, 1, 2, \ldots)$. The Parity Lemma implies $2|V_n(2a,-1)$, since $2a$ is even.

**5. Solutions of Pell equations with $d = a^2 \pm 1$ and $c = \pm 4$.**

In this section we consider solutions of Pell equations of the form $x^2 - (a^2 \pm 1)y^2 = \pm 4$.

**Lemma 5.1.** *If $2 \le a$, $a \ne 3$ and $x^2 - (a^2 - 1)y^2 = \pm 4$, then $y$ is even.*

**Proof.** Let $d = a^2 - 1$. Suppose $2 \le a$, $a \ne 3$ and $x^2 - dy^2 = \pm 4$. If $a$ is even, then $4|a^2$ and so $d \equiv -1 \pmod 4$. Hence $x^2 - dy^2 = \pm 4 \Rightarrow x^2 + y^2 \equiv 0 \pmod 4 \Rightarrow y \equiv x \equiv 0 \pmod 2$. Therefore we can suppose $a$ is odd and $5 \le a$. Then $4|d$ and so $x$ is even. Suppose $y$ is odd, and without loss of generality that $y$ is the least such odd $y > 0$. Since $3 < a$, $(a-1)^2 < a^2 - 5 < a^2 + 3 < (a+1)^2$. Hence $d \pm 4$ is not a square and so $y \ne 1$. Therefore $2 < y$. Let $x' = ax - dy$ and $y' = ay - x$. Then

$$x'^2 - dy'^2 = (ax - dy)^2 - d(ay - x)^2 = (a^2 - d)x^2 - d(a^2 - d)y^2 = x^2 - dy^2 = \pm 4.$$

Hence $(x', y')$ is also a solution. Since $x$ is even and $a$ and $y$ are both odd, $y'$ is odd. Now $5 \le a$ and $2 < y \;\Rightarrow 2y^2(1-a) < \pm 4 < y^2 \iff$

$$2y^2 - 2ay^2 < \pm 4 < y^2 \iff y^2 - 2ay^2 < -y^2 \pm 4 < 0 \iff$$
$$a^2y^2 - 2ay^2 + y^2 < a^2y^2 - y^2 \pm 4 < a^2y^2 \iff$$
$$(a^2 - 2a + 1)y^2 < (a^2 - 1)y^2 \pm 4 < a^2y^2 \iff$$
$$(a-1)^2y^2 < x^2 < a^2y^2 \iff (a-1)y < x < ay \iff$$

$0 < ay - x < y \iff 0 < y' < y$. But since $x'^2 - dy'^2 = \pm 4$ and $y'$ is odd, this contradicts the choice of $y$. Hence no such odd $y$ exists.

**Lemma 5.2.** *If $1 \le a$, $a \ne 2$ and $x^2 - (a^2 + 1)y^2 = \pm 4$, then $y$ is even.*

**Proof.** Let $d = a^2 + 1$. Suppose $1 \le a$, $a \ne 2$ and $x^2 - dy^2 = \pm 4$. If $a$ is odd, then $a^2 \equiv 1 \pmod 4$ and so $d \equiv 2 \pmod 4$. Hence $x^2 - dy^2 = \pm 4 \Rightarrow x^2 + 2y^2 \equiv 0 \pmod 4 \Rightarrow y \equiv x \equiv 0 \pmod 2$. Consequently we can suppose $a$ is even and since $a \ne 2$, that $4 \le a$. Suppose $y$ is odd and $y$ is the least such odd $y > 0$. Since $d$ is odd and $y$ is odd, $x$ must be odd. Since $2 < a$, $(a-1)^2 < a^2 - 3 < a^2 + 5 < (a+1)^2$ so that $d \pm 4$ is not a square and hence $y \ne 1$. Thus $2 < y$. Put $x' = dy - ax$ and $y' = x - ay$. As in the proof of Lemma 5.1, $x'^2 - dy'^2 = \pm 4$. Since $y' = x - ay$, $x$ is odd and $a$ is even, $y'$ is odd. Now $2 < a$ and $2 < y \;\Rightarrow -y^2 < \pm 4 < 2ay^2 \iff 0 < y^2 \pm 4 < 2ay^2 + y^2 \iff$

$$a^2y^2 < a^2y^2 + y^2 \pm 4 < a^2y^2 + 2ay^2 + y^2 \iff$$
$$a^2y^2 < (a^2 + 1)y^2 \pm 4 < (a+1)^2y^2 \iff$$
$$a^2y^2 < x^2 < (a+1)^2y^2 \iff ay < x < (a+1)y \iff$$

$0 < x - ay < y \iff 0 < y' < y$. But since $x'^2 - dy'^2 = \pm 4$ and $y'$ is odd, this contradicts the choice of $y$. Hence no such odd $y$ exists.

**Theorem 5.3.** *If $2 \le a$ and $a \ne 3$, then all solutions of $x^2 - (a^2-1)y^2 = +4$ are given by $x = V_i(2a, +1)$ and $y = 2U_i(2a, +1)$, $(i = 0, 1, 2, \ldots)$.*

**Proof.** Suppose $2 \le a$, $a \ne 3$ and $x^2 - (a^2-1)y^2 = +4$. By Lemma 5.1, $2|y$. Let $y = 2u$. $x^2 - (a^2-1)y^2 = +4 \iff x^2 - (a^2-1)4u^2 = +4 \iff x^2 - ((2a)^2 - 4)u^2 = +4 \iff x = V_i(2a, +1)$ and $u = U_i(2a, +1)$ for some $i$, by Corollary 2.7, since $4 \le 2a$.

**Theorem 5.4.** *If $1 \le a$ and $a \ne 2$, then all solutions of $x^2 - (a^2+1)y^2 = +4$ are given by $x = V_{2i}(2a, -1)$ and $y = 2U_{2i}(2a, -1)$, $(i = 0, 1, 2, \ldots)$.*

**Proof.** Suppose $1 \le a$, $a \ne 2$ and $x^2 - (a^2+1)y^2 = +4$. By Lemma 5.2, $2|y$. Let $y = 2u$. $x^2 - (a^2+1)y^2 = +4 \iff x^2 - (a^2+1)4u^2 = +4 \iff x^2 - ((2a)^2 + 4)u^2 = +4 \iff x = V_{2i}(2a, -1)$ and $u = U_{2i}(2a, -1)$ for some $i$, $(i = 0, 1, \ldots)$, by Corollary 2.9, since $1 \le 2a$.

**Theorem 5.5.** *If $1 \le a$ and $a \ne 2$, then all solutions of $x^2 - (a^2+1)y^2 = -4$ are given by $x = V_{2i+1}(2a, -1)$ and $y = 2U_{2i+1}(2a, -1)$, $(i = 0, 1, 2, \ldots)$.*

**Proof.** Suppose $1 \le a$, $a \ne 2$ and $x^2 - (a^2+1)y^2 = -4$. By Lemma 5.2, $2|y$. Let $y = 2u$. $x^2 - (a^2+1)y^2 = -4 \iff x^2 - (a^2+1)4u^2 = -4 \iff x^2 - ((2a)^2 + 4)u^2 = -4 \iff x = V_{2i+1}(2a, -1)$ and $u = U_{2i+1}(2a, -1)$ for some $i$, $(i = 0, 1, \ldots)$, by Corollary 2.8, since $1 \le 2a$.

**Theorem 5.6.** *If $2 \le a$ and $a \ne 3$, then $x^2 - (a^2-1)y^2 = -4$ has no solutions.*

**Proof.** Suppose $2 \le a$, $a \ne 3$ and $x^2 - (a^2-1)y^2 = -4$. By Lemma 5.1, $2|y$. Let $y = 2u$. Then $x^2 - (a^2-1)y^2 = -4 \Rightarrow x^2 - (a^2-1)4u^2 = -4 \Rightarrow x^2 - ((2a)^2 - 4)u^2 = -4$. But this equation has no solutions by Corollary 2.6, since $4 \le 2a$.

## References


[1] Davis, M., Hilbert's tenth problem is unsolvable, *Amer. Math. Monthly*, **80** (1973), 233–269.

[2] Davis, M., Matijasevich, Y., V. and Robinson, J., Hilbert's tenth problem. Diophantine equations: Positive aspects of a negative solution, Mathematical developments arising from Hilbert problems, *Proc. of Symposia in Pure Math.*, **28**, Amer. Math. Soc., Providence, Rhode Island, (1976), 323–378.

[3] Davis, M., Putnam, H. and Robinson, J., The decision problem for exponential diophantine equations, *Annals of Math.*, Series 2, **74** (1961), 425–436.

[4] Jones, J. P., Diophantine representation of the Fibonacci numbers, *Fibonacci Quarterly,* **13** (1975), 84–88.

[5] Jones, J. P., Satao, D., Wada, H. and Wiens, D., Diophantine representation of the set of prime numbers, *Amer. Math. Monthly*, **83** (1976), 449–464.

[6] Jones, J. P., Diophantine representation of Mersenne and Fermat primes, *Acta Arithmetica*, **35** (1979), 209–221.

[7] Jones, J. P., Universal diophantine equation, *Jour. Symbolic Logic*, **47** (1982), 549–571.

[8] Jones, J. P. and Matiyasevich, Y. V., A New Representation for the Symmetric Binomial Coefficient and its Applications, *Annales des Sciences Mathematiques du Quebec*, **6** (1982), 81–97.

[9] Jones, J. P. and Matiyasevich, Y. V., *Exponential Diophantine Representation of Recursively Enumerable Sets*, Proceedings of the Herbrand Symposium, Logic Colloquium 1981, Marseilles, France. Studies in Logic, Vol. 107, North Holland Publishers, Amsterdam, 1982, 159–177.

[10] Jones, J. P. and Matiyasevich, Y. V., Proof of recursive unsolvability of Hilbert's Tenth Problem, *Amer. Math. Monthly*, **98** (1991), 689–709.

[11] Kiss, P. and Jones, J. P., Some diophantine approximation results concerning second order linear recurrences, *Math. Slovaca*, **42** (1992), No. 5, 583–591.

[12] Jones, J. P. and Kiss, P., On points whose coordinates are terms of a linear recurrence, *Fibonacci Quarterly,* **31** (1993), 239–245.

[13] Jones, J. P. and Kiss, P., Some identities and congruences for a special family of second order recurrences, *Acta Academiae Paedagogicae Agriensis, New Series,* **23** (1995-96), 3–9.

[14] Jones, J. P. and Kiss, P., Some congruences concerning second order recurrences, *Acta Academiae Paedagogicae Agriensis, New Series*, **24** (1997), 29–33.

[15] Kiss, P. and Jones, J. P., Some new identities and congruences for Lucas sequences, *Discussiones Math.*, **18** (1998), 39–47.

[16] Kiss, P., A diophantine approximative property of second order linear recurrences, *Period. Math.*, **11** (1980), 281–287.

[17] Kiss, P., Diophantine representation of generalized Fibonacci numbers, *Elemente der Mathematik,* **34** (1979), 129–132.

[18] Lehmer, D. H., On the multiple solutions of the Pell Equation, *Annals of Math.*, **30** (1928), 66–72.

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

[20] Lucas, E., Sur les congruences des nombres euleriens et des coefficients differentiels des fonctions trigonom triques suivant un module premier, *Bulletin de la Societe Mathematique de France*, **6** (1877–78), 49–54.

[21] Lucas, E., Theorie des fonctions numeriques simplement periodiques, *Amer. Jour. of Math.*, **1** (1878), 184–240, 289–321. English translation: Fibonacci Association, Santa Clara University, 1969.

[22] Matiyasevich, Y. V., Enumerable sets are diophantine, *Doklady Akademii Nauk SSSR,* **191** (1970), 279–282 (Russian). English transl. Soviet Math. Doklady **11** (1970), 354–357.

[23] Yuri Matiyasevich and Julia Robinson, Reduction of an arbitrary diophantine equation to one in 13 unknowns, *Acta Arithmetica*, **27** (1975), 521–553.

[24] Yuri Matiyasevich, Algorithmic unsolvability of exponential diophantine equations in three unknowns, *Studies in the Theory of Algorithms and Mathematical Logic, Akad. Nauk.*, Moscow, (1979), 69–78.

[25] Yuri V. Matiyasevich, *Hilbert's Tenth Problem,* Foundations of Computing series, M. I. T. Press, Cambridge, Massachusetts, 1993.

[26] Julia Robinson, Existential definability in arithmetic, *Trans. Amer. Mathematical Society,* **72** (1952), 437–449.

[27] Julia Robinson, Diophantine decision problems, *Studies in Number Theory (W. J. LeVeque, ed.), MAA Studies in Mathematics*, **6** (1969), 76–116.

[28] Julia Robinson, Unsolvable diophantine problems, *Proc. Amer. Math. Soc.*, **22** (1969), 534–538.

[29] Sun Zhiwei, *Singlefold diophantine representation of the sequence* $u_0 = 0$, $u_1 = 1$ *and* $u_{n+2} = m \cdot u_{n+1} + u_n$, Pure and Applied Logic (Zhang Jinwen ed.), Beijing University Press, (1992), 97–101.



**James P. Jones**
University of Calgary
Department of Mathematics and Statistics
Calgary Alberta, T2N1N4 Canada
e-mail: jpjones@math.ucalgary.ca