#A15 INTEGERS 12A (2012): John Selfridge Memorial Issue

EXPLICIT SOLUTIONS OF CERTAIN SYSTEMS OF PELL EQUATIONS

Paulo Ribenboim
Department of Mathematics and Statistics, Queen's University, Kingston, Ontario, Canada
mathstat@mast.queensu.ca

Received: 12/23/10, Revised: 8/22/11, Accepted: 11/13/11, Published: 10/12/12

Abstract

We show how to obtain the solutions of families of systems of two Pell equations; these families are parameterized by the prime numbers.

-Dedicated to the memory of John Selfridge.
His opera voice is no more, but his voice in mathematics will continue to be heard, powerful.

1. Preliminaries

In recent years one finds several articles dedicated to simultaneous Pell equations, especially by Bennet and Walsh.

In this paper we apply an algorithm introduced in [11] to obtain explicit solutions for certain types of systems of Pell equations which were not considered previously by other authors.

Let $F > 1$ and let $\epsilon = c + d\sqrt{F}$ be the fundamental unit of $\mathbb{Z}[\sqrt{F}]$, let $P = 2c$ and $Q = c^2 - d^2F = \pm 1$. We also define

$$\epsilon' = c' + d'\sqrt{F} = \begin{cases} \epsilon & \text{if } Q = 1 \\ \epsilon^2 & \text{if } Q = -1. \end{cases}$$

Let $U_n = U_n(P,Q)$ and $V_n = V_n(P,Q)$ be the terms of the Lucas sequences with parameters (P,Q). We note that V_n is even, $V_{2n} \equiv 2 \pmod 4$ and

$$\epsilon^n = \frac{V_n}{2} + dU_n\sqrt{F}$$

for every $n \in \mathbb{Z}$.

Let f be a nonzero integer and $\delta = |f|/f$. If a and b are integers satisfying $a^2 - Fb^2 = f$ and such that

$$0 \le a \le \sqrt{\frac{(c'+\delta)|f|}{2}} \qquad \text{and} \qquad 0 \le b \le d'\sqrt{\frac{|f|}{2(c'+\delta)}},$$

we say that (a,b) is a fundamental solution of the Pell equation

$$x^2 - Fy^2 = f. \tag{1}$$

If $n \ge 0$, we write $x_n + y_n\sqrt{F} = (a + b\sqrt{F})\epsilon^n$ (x_n and y_n depend on (a,b), but this need not be expressed in the notation). Nagell ([8], [9]) proved that if $x > 0$ and $y > 0$ and if $x^2 - Fy^2 = f$ there exists a fundamental solution (a,b) and $n \ge 0$ such that $Q^n = 1$ and $x = x_n$, $y = y_n$. Then

$$\begin{cases} x_n = a\dfrac{V_n}{2} + bdFU_n \\[2ex] y_n = adU_n + b\dfrac{V_n}{2}. \end{cases}$$

If $s \ge 1$ let

$$\begin{aligned} k_s &= \tfrac{1}{4}(2 + Q^s V_{2s}), \\ h_s &= \tfrac{1}{4}(2 - Q^s V_{2s}), \end{aligned}$$

so k_s, h_s are integers, different from 0 and 1, and $k_s + h_s = 1$. For every $s \ge 1$ and $n > s$ with $Q^n = 1$ we have the relations

$$x_n^2 - Fy_{n-s}y_{n+s} = fk_s \tag{2}$$

$$x_n^2 - x_{n-s}x_{n+s} = fh_s. \tag{3}$$

Relation (2) was proved in [11] and the proof of (3) is similar.

The following theorem was proved in [11]:

Theorem 1. *Let $F > 1$, $G \ge 1$ be square-free integers, let $f \ne 0$ and $s \ge 1$ be integers, let $g = fk_s$ or fh_s. Then there exists an effectively computable integer $N > 0$, depending on F, G, f and s, such that if $x \ge 0$, $y \ge 0$, $z > 0$ and $p = 1$ or p is a prime number, and if*

$$\begin{cases} x^2 - Fy^2 = f \\ x^2 - pGz^2 = g, \end{cases} \tag{4}$$

then $x, y, z, p < N$.

The proof of the theorem implies a method which in many cases allows one to determine explicitly the solutions of (1). In [11] we gave a numerical example to illustrate the method. Our purpose here will be to give more examples and to discuss the short-comings of the method.

2. The Original Example of Ljunggren

In the papers [3], [4], [5] and [6] Ljunggren studied among others, the equation

$$x^4 - Fy^2 = 1,$$

where $F > 1$ is square-free. When F is a prime number, Ljunggren proved the result in example 1. Our method of proof is very natural, but to be fair to Ljunggren, it can be considered as a streamlined reformulation of his proof.

Example 1. If p is a prime number, if $x \geq 0$ and $y > 0$ are integers such that

$$x^4 - py^2 = 1 \tag{5}$$

then $(x, y, p) = (3, 4, 5)$ or $(99, 1920, 29)$.

Proof. We have $(x^2-1)(x^2+1) = x^4 - 1 = py^2$ with $d = \gcd(x^2-1, x^2+1) = 1$ or 2. If $d = 1$ then $x^2 - 1$ or $x^2 + 1$ is a square, which is impossible. If $d = 2$ we have one of the following cases:

$$\text{Case 1: } x^2 + 1 = 2\square \text{ and } x^2 - 1 = 2p\square$$
$$\text{Case 2: } x^2 - 1 = 2\square \text{ and } x^2 + 1 = 2p\square$$

These cases lead respectively to the systems below.

$$\text{Case 1} \begin{cases} x^2 - 2y^2 = -1 \\ x^2 - 2pz^2 = 1 \end{cases} \tag{6}$$

$$\text{Case 2} \begin{cases} x^2 - 2y^2 = 1 \\ x^2 - 2pz^2 = -1 \end{cases} \tag{7}$$

The fundamental unit of $\mathbb{Z}[\sqrt{2}]$ is $\epsilon = 1 + \sqrt{2}$, so $P = 2$, $Q = -1$ and U_n and V_n are the Pell numbers. Because $k_1 = -1$, the systems may be treated in both cases by our method.

`Case 1.` The fundamental solution of the first equation is ϵ, so its solutions are among

$$x_n + y_n\sqrt{2} = \epsilon^{n+1} = \frac{V_{n+1}}{2} + U_{n+1}\sqrt{2}$$

with n such that $Q^n = 1$, that is, n even. By relation (2), we have $2y_{n-1}y_{n+1} = 2p\square \neq 0$, so $U_nU_{n+2} = p\square$. We have $\gcd(U_n, U_{n+2}) = 2$, hence either (a) $U_n = 2\square$, $U_{n+2} = 2p\square$ or (b) $U_n = 2p\square$, $U_{n+2} = 2\square$. But the Pell number $U_m = 2\square$ exactly when $m = 2$, so (a) and (b) are impossible.

`Case 2.` The fundamental solution of the first equation is ϵ^2, so

$$x_n + y_n\sqrt{2} = \epsilon^{n+2} = \frac{V_{n+2}}{2} + U_{n+2}\sqrt{2}.$$

By the relation (2), we have $2y_{n-1}y_{n+1} = 2p\Box$, so $U_{n+1}U_{n+3} = p\Box$ with $\gcd(U_{n+1}, U_{n+3}) = 1$ because n is even. As proved by Ljunggren, $U_m = \Box$ if and only if $m = 1, 7, -1, -7$. We have two cases: (a) $U_{n+1} = \Box$, $U_{n+3} = p\Box$ or (b) $U_{n+1} = p\Box$, $U_{n+3} = \Box$.

In case (a), we have $n = 0$, so $x_0 = V_2/2 = 3$, $y_0 = -U_2 = 2$, $p = 5$. This leads to the solution $(x, y, p) = (3, 4, 5)$ of equation (5).

In case (b), we have $n = 4$, so $x_4 = V_6/2 = 99$, $y_4 = U_6 = 70$, $p = 29$. This leads to the solution $(x, y, p) = (99, 1920, 29)$ of equation (5). This completes the proof. $\Box$

In contrast the proof of Ljunggren appealed to the solution of the equations $h^4 - 2k^4 = \pm 1$ considered earlier by Mordell [7].

3. Numerical Examples

Let F, G, f, s, k_s, h_s and $g = fk_s$ or fh_s be as indicated earlier. We shall use the notation $\langle F, f|G, g\rangle$ to denote the family of systems (4), where $p = 1$ or p is a prime number.

Our purpose is to find all solutions (x, y, z, p), with $x \geq 0$, $y \geq 0$, $z > 0$, p; for each solution, it suffices to give the pair (x, p) since y and z are then uniquely determined.

If there exists an integer m such that $\langle F, f|G, g\rangle$ has no solution modulo m, then $\langle F, f|G, g\rangle$ has no solution in integers. Other simple sufficient conditions are the following: (a) If there exists an integer m dividing G such that $F(g - f) \not\equiv \Box \pmod{m}$, then $\langle F, f|G, g\rangle$ has no solution; and (b) Given $p_0 = 1$ or a prime, if there exists an integer m dividing F such that $G(f - g) \not\equiv p_0\Box \pmod{m}$, then $\langle F, f|G, g\rangle$ has no solution with $p = p_0$. The reader may verify easily that there are no solutions in the following examples: $\langle 2, 1|1, -1\rangle$, and $\langle 2, 2|1, -2\rangle$ (this can be seen in both cases by, e.g., reducing modulo 2 and then modulo 4).

We shall give an example where $\langle F, f|G, g\rangle$ has no solution in integers, but has a solution modulo every prime q.

Example 2. The family of systems $\langle 2, 1|3, 9\rangle$ has no solution in integers, but has a solution modulo every prime q.

Proof. For every prime q, $(3, 2, q, p)$ is a solution modulo q. Now we show that $\langle 2, 1|3, 9\rangle$ has no solution.

With the method used in §2, and the same notation, $\epsilon = 1 + \sqrt{2}$, $P = 2$, $Q = -1$ and U_n and V_n are the Pell numbers. The fundamental solution of $x^2 - 2y^2 = 1$ is $\epsilon^2 = 3 + 2\sqrt{2}$:

$$x_n + y_n\sqrt{2} = \epsilon^{n+2} = \frac{V_{n+2}}{2} + U_{n+2}\sqrt{2}. \tag{8}$$

We note that $k_2 = \frac{1}{4}(2 + Q^2V_4) = 9$. By relation (2), $2y_{n-2}y_{n+2} = 3pz^2$, so $U_nU_{n+4} = 3p\square$. From $Q^n = 1$, it follows that n is even, and $d = \gcd(U_n, U_{n+4}) = 2$ or 12. Also, if $p = 2$ then $U_nU_{n+4} = 3\square$, while if $p \neq 2$, then $U_nU_{n+4} = 6p\square$. We recall that n is even, so $U_n \neq \square$, $U_{n+4} \neq \square$; also $U_m = 2\square$ if and only if $m = 2$. In [11] we proved that $U_m = 3\square$ if and only if $m = 4$; moreover, $U_n \neq 6\square$ for all m.

We examine the possible cases.

First, let $p = 2$, so $U_nU_{n+4} = 3\square$. If $d = 2$,

$$\begin{cases} U_n = 6\square \\ U_{n+4} = 2\square \end{cases} \left| \begin{array}{l} 2\square \\ 6\square \end{array} \right.$$

and both cases are impossible. If $d \neq 2$,

$$\begin{cases} U_n = \square \\ U_{n+4} = 3\square \end{cases} \left| \begin{array}{l} 3\square \\ \square \end{array} \right.$$

and again both cases are impossible.

Now let $p \neq 2$, so $U_nU_{n+4} = 6p\square$. If $d = 2$, then $n \equiv 2 \pmod 4$, $\frac{U_n}{2} \cdot \frac{U_{n+4}}{2} = 6p\square$. From what was said above, all cases are immediately excluded since $3 \nmid U_n$ and $3 \nmid U_{n+4}$. If $d = 12$, from what was said above the only possibilities are

$$\begin{cases} U_n = 2p\square \\ U_{n+4} = 3\square \end{cases} \left| \begin{array}{l} 3\square \\ 2p\square \end{array} \right.$$

This gives $n = 0$, respectively $n = 4$, and both are impossible. $\square$

The next example has solutions, which we shall determine explicitly.

Example 3. The solutions of $\langle 2, -1 | 2, -9 \rangle$ are $(x, p) = (7, 29), (1393, 5741), (1, 5), (41, 5)$.

Proof. Once again, $\epsilon = 1 + \sqrt{2}$ is the fundamental solution of the first equation, $P = 2$, $Q = -1$ and U_n, V_n are the Pell numbers. Our method is applicable, since $k_2 = 9$. We have

$$x_n + y_n\sqrt{2} = \frac{V_{n+1}}{2} + U_{n+1}\sqrt{2}$$

and $2y_{n-2}y_{n+2} = 2p\square$, so $U_{n-1}U_{n+3} = p\square$, with n even. Since $\gcd(n-1, n+3) = \gcd(U_{n-1}, U_{n+3}) = 1$, we have

$$\begin{cases} U_{n-1} = p\square \\ U_{n+3} = \square \end{cases} \left| \begin{array}{l} \square \\ p\square. \end{array} \right.$$

Let (1) and (2) respectively denote the subcases to the left and right of the vertical bar in the above displayed pair of equations.

Subcase (1): $n + 3 = -7, -1, 1$ or 7, so $n - 1 = -11, -5, -3, 3$. We have the possibilities:

n	p	x_n
-10	29	$V_{-9}/2=-1393$
-4	29	$V_{-3}/2=-7$
-2	5	$V_{-1}/2=-1$
4	5	$V_5/2=41$

Subcase (2): $n-1=-7,-1,1,7$, so $n+3=-3,3,5,11$. As before:

n	p	x_n
-6	5	$V_{-5}/2=-41$
0	5	$V_1/2=1$
2	29	$V_3/2=7$
8	5741	$V_9/2=1393$

□

The application of our method to other systems leads often to other special problems, not yet settled in the literature, about Pell numbers. We invite the reader to complete the details in the following example.

Example 4. The solutions of $\langle 2,1|2,-49\rangle$ are $(x,p)=(3,29),(99,197),(17,1),(1,5),(3363,33461)$.

Once again it is a question of Pell numbers. In the present example the following facts are needed: (a) $U_m=5\square$ if and only if $m=3$ or -3, and (b) $U_m=70\square$ if and only if $m=6$.

These facts are not present in the literature, but may be proved with the algorithm described in Ribenboim [10]. The method may be successfully applied when the following conditions are present.

(1) $f=\pm1$: In this case the fundamental solution of $x^2-Fy^2=\pm1$ is ϵ or ϵ^2. Then $x_n+y_n\sqrt{F}=\frac{V_{n+1}}{2}+dU_{n+1}\sqrt{F}$ or $\frac{V_{n+2}}{2}+dU_{n+2}\sqrt{F}$; so this leads to the determination of indices m such that U_m, or V_m is of the form $A\square$, for some square-free integer A.

(2) $f=\pm F$: Now $F\mid x$, let $x=Ft$, hence $y^2-Ft^2=\mp1$. Proceeding as in (1), $y_n+t_n\sqrt{F}=\frac{V_{n+1}}{2}+dU_{n+1}\sqrt{F}$ or $\frac{V_{n+2}}{2}+dU_{n+2}\sqrt{F}$, hence $y_n=\frac{V_{n+1}}{2}$ or $\frac{V_{n+2}}{2}$, $x_n=dFU_{n+1}$ or $x_n=dFU_{n+1}$.

(3) If $\epsilon=c+d\sqrt{F}$, it is required to know the indices n such that $U_n(2c,\pm1)=\square$ or $2\square$. The algorithm in [10] amounts to finding integral points in certain quartic models of elliptic curves. It makes it possible to determine the integers m such that $U_m(2c,\pm1)=A\square$, where A is a square-free integer. The knowledge of the integers n such that $V_n(2c,\pm1)=\square$ or $2\square$ may also be reached by our method. However, if $A\geq3$ is square-free the method presented here has not been successful to determine the indices n such that $V_n(2c,\pm1)=A\square$. Bennet and Walsh studied the equation $b^2x^4-dy^2=1$ where $b>1$, b square-free and they showed that this equation has at most one solution. In particular, they determined the indices n such that

$V_n(2c, 1) = A\square$, where $A \geq 3$, A is square-free. Their method used linear forms in logarithms of algebraic numbers, properties of Pell equations and the explicit determination of integral points on certain elliptic curves. See [1].

We inform the readers of the following results concerning sequences with parameters $P = 2c$, $Q = \pm 1$. For Pell numbers, Ljunggren proved [5]:

$$\begin{aligned}
&\{n \mid U_n = \square\} = \{-7, -1, 1, 7\},\\
&\{n \mid U_n = 2\square\} = \{2\},\\
&\{n \mid V_n = \square\} = \emptyset,\\
&\{n \mid V_n = 2\square\} = \{0, 1\}.
\end{aligned}$$

Ljunggren [5] and Cohn [2] proved:

$$\begin{aligned}
&\{n \mid U_n(4, -1) = \square\} = \{-1, 1, 2\},\\
&\{n \mid U_n(4, -1) = 2\square\} = \{4\},\\
&\{n \mid V_n(4, -1) = \square\} = \{1\},\\
&\{n \mid V_n(4, -1) = 2\square\} = \{-2, 0, 2\}.
\end{aligned}$$

Cohn [2] also determined squares and double-squares for other sequences. Let $2c \in \{V_m(A, -1) \mid A \geq 1, A \text{ odd}, m \equiv 3 \pmod 6, m > 0\}$. For $n \geq 0$, we have:

- $U_n(2c, -1) = \square$ if and only if $n = 1$; or $n = 2$ and $2c = V_3(1, -1) = 4$; or $n = 2$ and $2c = V_3(3, -1) = 36$.
- $U_n(2c, -1) = 2\square$ if and only if $n = 4$ and $2c = V_3(1, -1) = 4$.
- $V_n(2c, -1) = \square$ if and only if $n = 1$ and $2c = V_3(1, -1) = 4$; or $n = 1$, $2c = V_3(3, -1) = 36$.
- $V_n(2c, -1) = 2\square$ if and only if $n = 0$; or $n = 2$, $2c = V_3(1, -1) = 4$; or $n = 2$ and $2c = V_3(5, -1) = 140$.

For numbers $2c \in \{V_m(A, 1) \mid 3 \text{ divides } m, A \geq 1, A \text{ odd}\}$, we have:

- $U_n(2c, 1) = \square$ if and only if $n = 1$.
- $U_n(2c, 1) = 2\square$ if and only if $n = 2$, $2c = V_3(3, 1) = 18$; or $n = 2$, $2c = V_3(27, 1) = 19602$.
- $V_n(2c, 1) = \square$ is impossible.
- $V_n(2c, 1) = 2\square$ if and only if $n = 0$; or $n = 1$, $2c = V_3(3, 1) = 18$; or $n = 1$, $2c = V_3(27, 1) = 19602$.

References

[1] Bennet, M.A. and Walsh, G., The diophantine equation $b^2x^4 - dy^2 = 1$, Proc. Amer. Math. Soc. **127** (1999), 3481-3491.

[2] Cohn, J.H.E., Squares in some recurrent sequences, Pacific J. Math. **41** (1972), 631-646.

[3] Ljunggren, W., Einige Eigenschaften der Einheiten reeller quadratischer und rein biquadratischer Zahlkörper mit Anwendung auf die Lösung eine Klasse unbestimmter Gleichungen vierten Grades[1], Det Norske Vid. Akad. Skr. **12**, 1937.

[4] Ljunggren, W., Über die Gleichung $x^4 - Dy^2 = 1$, Archiv f. Math. og Naturvid. **45** (1942), 631-646.

[5] Ljunggren, W., Zur Theorie der Gleichung $x^2 + 1 = Dy^4$, Det Norske Vid. Akad. Skr. (1942).

[6] Ljunggren, W., Some remarks on the diophantine equations $x^2 - Dy^4 = 1$ and $x^4 - Dy^2 = 1$, J. London Math. Soc. **41** (1965), 42-44.

[7] Mordell, L.J., The diophantine equation $y^2 = Dx^4 + 1$, J. London Math. Soc. **34** (1964), 161-164.

[8] Nagell, T., Über die Darstellung ganzer Zahlen durch eine indefinite bilinäre quadratische Form[2], Archiv d. Math. **2** (1949/50), 161-165.

[9] Nagell, T., Bemerkung[2] über die Diophantische Gleichung $u^2 - Dv^2 = c$, Archiv d. Math. **3** (1952), 8-9.

[10] Ribenboim, P., An algorithm to determine the points with integral coordinates in certain elliptic curves, J. Number Theory **74** (1999), 19-38.

[11] Ribenboim, P., Solving parametrized systems of Pell equations, Acta Arith. **113** (2005), 1-9.

[1]Reprinted in *Collected Papers of Wilhelm Ljunggren* (editor Paulo Ribenboim), Queen's Papers in Pure and Applied Mathematics, Vol. 115, 2003, Kingston

[2]Reprinted in *Collected Papers of Tryque Nagell* (editor Paulo Ribenboim), Queen's Papers in Pure and Applied Mathematics, vol. 121, 2002, Kingston