PELL'S EQUATION AND PELL NUMBER TRIPLES

M. J. DE LEON
Florida Atlantic University, Boca Raton, Florida 33432

The Pell numbers are defined by

$$P_0 = 0, \quad P_1 = 1, \quad \text{and} \quad P_{n+2} = 2P_{n+1} + P_n \quad \text{for} \quad n \geq 0.$$

In [1] it was noted that if

$$p > q > 0 \quad \text{and} \quad p^2 - q^2 - 2pq = \pm N,$$

where N is a square or twice a square, then there exist non-negative integers a, b, and n with $a \geq b$ such that

$$p = aP_{n+2} - bP_{n+1} \quad \text{and} \quad q = aP_{n+1} - bP_n,$$

or

$$p = bP_{n+2} + aP_{n+1} \quad \text{and} \quad q = bP_{n+1} + aP_n .$$

We shall prove this result for $p \geq q \geq 0$ and $N > 1$ and, in addition, show that $(a+b)^2 - 2b^2 = N$ (Theorem 6). We shall also prove the converse of this result (Theorem 8). In order to prove Theorem 6 we shall need Theorem 2, which gives an interesting property of the fundamental solution(s) to Pell's Equation

(1) $$u^2 - Dv^2 = C,$$

where D is a positive integer which is not a perfect square and $C \neq 0$. The converse of Theorem 2 is also true but it is neither stated nor proved since it is not needed to prove Theorem 6.

Before proving these results we need to establish some definitions and theorems concerning (1). For this we can do no better than follow Nagel [2, 195–212] with but one exception.

If u and v are integers which satisfy (1), then we say $u + v\sqrt{D}$ is a solution to (1). If $u + v\sqrt{D}$ and $u^* + v^*\sqrt{D}$ are both solutions to (1) then they are called *associate solutions* iff there exists a solution $x + y\sqrt{D}$ to $x^2 - Dy^2 = 1$ such that

$$(u + v\sqrt{D}) = (u^* + v^*\sqrt{D})(x + y\sqrt{D}).$$

The set of all solutions associated with each other forms a class of solutions of (7). Every class contains an infinite number of solutions [2, 204].

It is possible to decide whether the two given solutions $u + v\sqrt{D}$ and $u^* + v^*\sqrt{D}$ belong to the same class or not. In fact, it is easy to see that the necessary and sufficient condition for these two solutions to be associated with each other is that the two numbers

$$\frac{uu^* - vv^*D}{C} \quad \text{and} \quad \frac{vu^* - uv^*}{C}$$

be integers.

If K is the class consisting of the solutions

$$u_i + v_i\sqrt{D}, \qquad i = 1, 2, 3, \cdots,$$

it is evident that the solutions

$$u_i - v_i\sqrt{D}, \qquad i = 1, 2, 3, \cdots,$$

also constitute a class, which may be denoted by $\bar{K}$. The classes K and $\bar{K}$ are said to be *conjugates* of each other. Conjugate classes are in general distinct, but may sometimes coincide; in the latter case we speak of *ambiguous* classes.

If the diophantine equation $u^2 - Dv^2 = C$ is solvable then from among all solutions $u + v\sqrt{D}$ in a given class K of solutions to $u^2 - Dv^2 = C$, we shall now choose a solution $u_0 + v_0\sqrt{D}$, which we shall call the *fundamental solution* of the class K. The manner of selecting this solution will depend on the value of C.

(i) For the case $C > 1$, let u_0 be the least positive value of u which occurs in K. If K is not ambiguous then the number v_0 is uniquely determined. If K is ambiguous we get a uniquely determined v_0 by prescribing that $v_0 \geqslant 0$.

(ii) For the case $C \leqslant -1$ or $C = 1$ let v_0 be the least positive value of v which occurs in K. If K is not ambiguous then the number u_0 is uniquely determined. If K is ambiguous we get a uniquely determined u_0 by prescribing that $u_0 \geqslant 0$.

In the sequel we shall always denote the fundamental solution of $u^2 - Dv^2 = 1$ by $x_1 + y_1\sqrt{D}$ instead of by $u_0 + v_0\sqrt{D}$. Since there is only one class of solutions to $u^2 - Dv^2 = 1$, we have that $x_1 > 0$ and $y_1 > 0$.

EXAMPLES. The fundamental solution to $u^2 - 2v^2 = 1$ is $3 + 2\sqrt{2}$. The fundamental solution to $u^2 - 2v^2 = -1$ is $1 + \sqrt{2}$. The two different classes of solutions to $u^2 - 2v^2 = 7$ have as their fundamental solutions $3 + \sqrt{2}$ and $3 - \sqrt{2}$. The four different classes of solutions to $u^2 - 2v^2 = 119$ have as their fundamental solution $11 + \sqrt{2}$, $11 - \sqrt{2}$, $13 + 5\sqrt{2}$, $13 - 5\sqrt{2}$.

REMARK A. It follows from the definition of fundamental solution that if $u_0 + v_0\sqrt{D}$ is a fundamental solution to a class K of solutions to $u^2 - Dv^2 = C$, where $C \neq 0$, then

(i) $$u_0 + v_0\sqrt{D} > 0,$$

(ii) for $C \neq 1$, if $u + v\sqrt{D}$ is in K then
$$|u| \geqslant |u_0| \quad \text{and} \quad |v| \geqslant |v_0|, \text{ and}$$

(iii) If $C \geqslant 1$ then $u_0 > 0$ and if $C \leqslant 1$ then $v_0 > 0$.

In (ii) we must exclude $C = 1$ since for $C = 1$, $u = 1$ and $v = 0$ is a solution to $u^2 - Dv^2 = 1$ but it is not the fundamental solution.

Our definition of fundamental solution differs from Nagel's only when $v_0 < 0$. In this case, while our fundamental solution is $u_0 + v_0\sqrt{D}$ his is $-(u_0 + v_0\sqrt{D})$. Instead of satisfying $u_0 + v_0\sqrt{D} > 0$ as our fundamental solutions do Nagel's satisfy $v_0 \geqslant 0$.

If $u_0 + v_0\sqrt{D}$ is a fundamental solution to a class K of solutions to $u^2 - Dv^2 = C$, we shall sometimes simply say that $u_0 + v_0\sqrt{D}$ is a fundamental solution to $u^2 - Dv^2 = C$.

Lemma 1. [2, 205–207]. Let $x_1 + y_1\sqrt{D}$ be the fundamental solution to $x^2 - Dy^2 = 1$. If $u_0 + v_0\sqrt{D}$ is a fundamental solution to the equation $u^2 - Dv^2 = -N$, where $N > 0$, then

$$0 < |v_0| \leqslant \frac{y_1\sqrt{N}}{\sqrt{2(x_1 - 1)}} \quad \text{and} \quad 0 \leqslant |u_0| \leqslant \sqrt{\tfrac{1}{2}(x_1 - 1)N}\,.$$

If $u_0 + v_0\sqrt{D}$ is a fundamental solution to the equation $u^2 - Dv^2 = N$, where $N > 1$, then

$$0 \leqslant |v_0| \leqslant \frac{y_1\sqrt{N}}{\sqrt{2(x_1 + 1)}} \quad \text{and} \quad 0 < |u_0| \leqslant \sqrt{\tfrac{1}{2}(x_1 + 1)N}\,.$$

Theorem 2. Let $x_1 + y_1\sqrt{D}$ be the fundamental solution to $x^2 - Dy^2 = 1$. If

$$k = \frac{y_1}{x_1 - 1}$$

and if $u_0 + v_0\sqrt{D}$ is a fundamental solution to $u^2 - Dv^2 = -N$, where $N > 0$, then $v_0 = |v_0| \geqslant k|u_0|$. If

$$k = \frac{Dy_1}{x_1 - 1}$$

and if $u_0 + v_0\sqrt{D}$ is a fundamental solution to $u^2 - Dv^2 = N$, where $N > 1$, then $u_0 = |u_0| \geqslant k|v_0|$.

Proof. Assume $u_0 + v_0\sqrt{D}$ is a fundamental solution to $x^2 - Dy^2 = -N$ and assume $|v_0| < k|u_0|$. Thus

$$-N = u_0^2 - Dv_0^2 > u_0^2 - Dk^2u_0^2 = u_0^2(1 - Dk^2).$$

Hence, by Lemma 1,

$$\frac{2u_0^2}{x_1 - 1} \leqslant N < u_0^2(Dk^2 - 1).$$

Therefore we have the contradiction

$$\frac{2}{x_1 - 1} < Dk^2 - 1 = \frac{Dy_1^2}{(x_1 - 1)^2} - 1 = \frac{x_1 + 1}{x_1 - 1} - 1 = \frac{2}{x_1 - 1} .$$

Now assume $u_0 + v_0\sqrt{D}$ is a fundamental solution to $u^2 - Dv^2 = N$ and assume $|u_0| < k|v_0|$. Thus

$$N = u_0^2 - Dv_0^2 < k^2v_0^2 - Dv_0^2 = (k^2 - D)v_0^2 .$$

Hence, by Lemma 1,

$$\frac{2(x_1 + 1)v_0^2}{y_1^2} \leqslant N < (k^2 - D)v_0^2 .$$

Therefore we have the contradiction

$$\frac{2(x_1 + 1)}{y_1^2} < k^2 - D = \frac{D[Dy_1^2 - (x_1 - 1)^2]}{(x_1 - 1)^2} = \frac{2D}{x_1 - 1} = \frac{2(x_1 + 1)}{y_1^2} .$$

Lemma 3. Let $u_0 + v_0\sqrt{D}$ be a fundamental solution to a class of solutions to $u^2 - Dv^2 = C$, where $C \neq 1$, and let $x + y\sqrt{D}$ be a solution to the equation $x^2 - Dy^2 = 1$. In addition, let

$$u + v\sqrt{D} = (u_0 + v_0\sqrt{D})(x + y\sqrt{D}).$$

If $u \geqslant 0$ and $v \geqslant 0$ then $x > 0$ and $y \geqslant 0$ (if $C = 1$, one requires $v > 0$ instead of $v \geqslant 0$).

Proof. Since $u_0 + v_0\sqrt{D} > 0$ and $u + v\sqrt{D} > 0$, $x + y\sqrt{D} > 0$. This implies $x > 0$. If $x = 1$ then $y = 0$ and the lemma is true. Thus assume $x > 1$. We need only show $y \geqslant 0$. Since $(x + y\sqrt{D})(x - y\sqrt{D}) = 1$, $y < 0$ implies $x + y\sqrt{D} < 1$. Whence

$$u + v\sqrt{D} = (u_0 + v_0\sqrt{D})(x + y\sqrt{D}) < u_0 + v_0\sqrt{D} .$$

This is impossible since, by Remark A, $u \geqslant u_0$ and $v \geqslant v_0$.

Lemma 4. [2, 197–198]. If $x + y\sqrt{D}$ is a solution, with $x > 0$ and $y \geqslant 0$, to the diophantine equation $x^2 - Dy^2 = 1$ then

$$(x + y\sqrt{D}) = (x_1 + y_1\sqrt{D})^m ,$$

where $x_1 + y_1\sqrt{D}$ is the fundamental solution to $x^2 - Dy^2 = 1$ and m is a non-negative integer.

If $u + v\sqrt{D}$ is a solution to the diophantine equation $u^2 - Dv^2 = C$ then, by the definition of a fundamental solution,

$$u + v\sqrt{D} = (u_0 + v_0\sqrt{D})(x + y\sqrt{D}),$$

where $u_0 + v_0\sqrt{D}$ is the fundamental solution to the class of solutions to $u^2 - Dv^2 = C$ to which $u + v\sqrt{D}$ belongs and $x^2 - Dy^2 = 1$. By Lemma 3, $u \geqslant 0$ and $v \geqslant 0$ imply $x > 0$ and $y \geqslant 0$. Hence by Lemma 4, we have

Theorem 5. If $u + v\sqrt{D}$ is a solution in non-negative integers to the diophantine equation $u^2 - Dv^2 = C$, where $C \neq 1$, then there exists a non-negative integer m such that

$$u + v\sqrt{D} = (u_0 + v_0\sqrt{D})(x_1 + y_1\sqrt{D})^m ,$$

where $u_0 + v_0\sqrt{D}$ is the fundamental solution to the class of solutions of $u^2 - Dv^2 = C$ to which $u + v\sqrt{D}$ belongs and $x_1 + y_1\sqrt{D}$ is the fundamental solution to $x^2 - Dy^2 = 1$.

Theorem 6. Let N be an integer greater than one. If $p \geqslant q \geqslant 0$ and $p^2 - q^2 - 2pq = \epsilon N$, where $\epsilon = 1$ or -1, then there exist non-negative integers a, b, n with $a \geqslant b$ such that either

(2) $$p = aP_{n+2} - bP_{n+1} \quad \text{and} \quad q = aP_{n+1} - bP_n ,$$

or

(3) $$p = bP_{n+2} + aP_{n+1} \quad \text{and} \quad q = bP_{n+1} + aP_n .$$

Also we have that $(a+b)^2 - 2b^2 = N$.

We shall now indicate how one can explicitly determine which of (2) or (3) is satisfied and also a, b, and n. Since $(p-q)^2 - 2q^2 = p^2 - q^2 - 2pq = \epsilon N$, by Theorem 5,

$$(4)\qquad (p-q) + q\sqrt{2} = (u_0 + v_0\sqrt{2})(3+2\sqrt{2})^m = u_m + v_m\sqrt{2}\ ,$$

where $u_0 + v_0\sqrt{2}$ is the fundamental solution to the class of solutions of $u^2 - 2v^2 = \epsilon N$ to which $(p-q) + q\sqrt{2}$ belongs and m is a non-negative integer.

If the product $\epsilon u_0 v_0$ is negative then p and q satisfy (2), where for $\epsilon = -1$ we have $a = v_0$, $b = v_0 - u_0$, $n = 2m$, and $a > b \geqslant 0$ whereas for $\epsilon = 1$ we have $a = u_0 + v_0$, $b = -v_0$, $n = 2m - 1$, $m \geqslant 1$, and $a \geqslant b > 0$.

If the product $\epsilon u_0 v_0$ is positive then p and q satisfy (3), where for $\epsilon = -1$ we have $a = v_0$, $b = u_0 + v_0$, $n = 2m-1$, $m \geqslant 1$, and $a > b \geqslant 0$ whereas for $\epsilon = 1$ we have $a = u_0 - v_0$, $b = v_0$, $n = 2m$, and $a \geqslant b > 0$.

If $u_0 = 0$ then p and q satisfy (2) for $a = v_0 = b$ and $n = 2m$. Furthermore, if $m \geqslant 1$ then p and q also satisfy (3) for $a = v_0 = b$ and $n = 2m - 1$.

If $v_0 = 0$ then p and q satisfy (3) for $a = u_0$, $b = 0$, and $n = 2m$. Furthermore, if $m \geqslant 1$ then p and q also satisfy (2) with $a = u_0$, $b = 0$, and $n = 2m - 1$.

In order to prove Theorem 6, we shall need

Lemma 7. Let $u_0 + v_0\sqrt{D}$ be a fundamental solution to $u^2 - 2v^2 = C$. For $m \geqslant 0$, let

$$u_m + v_m\sqrt{2} = (u_0 + v_0\sqrt{2})(3+2\sqrt{2})^m .$$

We have that

$$(5)\qquad u_m + v_m = v_0P_{2m+2} + (u_0 - v_0)P_{2m+1} = (u_0+v_0)P_{2m+1} + v_0P_{2m}$$

and

$$(6)\qquad v_m = v_0P_{2m+1} + (u_0 - v_0)P_{2m} = (u_0+v_0)P_{2m} + v_0P_{2m-1} .$$

Proof. The second equality in both (5) and (6) follows directly from $P_{n+2} = 2P_{n+1} + P_n$. We shall prove the first equality in both (5) and (6) by induction on m. Clearly (5) and (6) are true for $m = 0$. Thus assume (5) and (6) are true for $m = k$. Now

$$u_{k+1} + v_{k+1}\sqrt{2} = (u_k + v_k\sqrt{2})(3+2\sqrt{2}) = (3u_k + 4v_k) + (2u_k + 3v_k)\sqrt{2} .$$

Hence

$$\begin{aligned} u_{k+1} + v_{k+1} = 5u_k + 7v_k = 5(u_k + v_k) + 2v_k &= 5v_0P_{2k+2} + 5(u_0 - v_0)P_{2k+1} + 2v_0P_{2k+1} + 2(u_0 - v_0)P_{2k} \\ &= 5v_0P_{2k+2} + [5(u_0 - v_0) + 2v_0]P_{2k+1} + 2(u_0 - v_0)\ (P_{2k+2} - 2P_{2k+1}) \\ &= (u_0 + v_0)(2P_{2k+2} + P_{2k+1}) + v_0P_{2k+2} \\ &= (u_0 + v_0)P_{2k+3} + v_0P_{2k+2} = v_0P_{2k+4} + (u_0 - v_0)P_{2k+3} . \end{aligned}$$

Also

$$\begin{aligned} v_{k+1} &= 2v_k + 3v_k = 2(u_k + v_k) + v_k = 2[v_0P_{2k+2} + (u_0 - v_0)P_{2k+1}] + v_0P_{2k+1} + (u_0 - v_0)P_{2k} \\ &= 2v_0P_{2k+2} + 2u_0P_{2k+1} - v_0P_{2k+1} + (u_0 - v_0)(P_{2k+2} - 2P_{2k+1}) \\ &= (u_0 + v_0)P_{2k+2} + v_0P_{2k+1} = v_0P_{2k+3} + (u_0 - v_0)P_{2k+2} . \end{aligned}$$

Now we are ready for the

Proof of Theorem 6. Assume $p \geqslant q \geqslant 0$ and $p^2 - q^2 - 2pq = \epsilon N$. By (4) – (6), we have

$$(7)\qquad p = v_0P_{2m+2} + (u_0 - v_0)P_{2m+1} = (u_0 + v_0)P_{2m+1} + v_0P_{2m}$$

and

$$(8)\qquad q = v_0P_{2m+1} + (u_0 - v_0)P_{2m} = (u_0 + v_0)P_{2m} + v_0P_{2m-1} ,$$

where $u_0 + v_0\sqrt{2}$ is a fundamental solution to $u^2 - 2v^2 = \epsilon N$ and $m \geqslant 0$.

If $\epsilon u_0 v_0 < 0$ and $\epsilon = -1$ then let $a = v_0$, $b = v_0 - u_0$, and $n = 2m$. For this choice of a, b, and n, by (7) and (8), we have that (2) is satisfied. We also have that $a > b$, $b \geqslant 0$ (by Theorem 2 with $D = 2$) and $n \geqslant 0$.

If $\epsilon u_0 v_0 < 0$ and $\epsilon = 1$ then let $a = u_0 + v_0$, $b = -v_0$, and $n = 2m - 1$. For this choice of a, b, and n, we have that (2) is satisfied. We also have that $a \geqslant b$ (by Theorem 2), and $b > 0$. Finally $m \neq 0$ since $m = 0$ implies, by (4), the contradiction $q = v_0 < 0$. Thus $m \geqslant 1$.

The proof for $\epsilon u_0 v_0 \geqslant 0$ and the verification that $(a+b)^2 - 2b^2 = N$ are left to the reader.

Theorem 8. If p and q are integers which satisfy (2) or (3) with $n \geqslant 0$, $a \geqslant b \geqslant 0$, and $(a+b)^2 - 2b^2 = N$, then $p \geqslant q \geqslant 0$ and $p^2 - q^2 - 2pq = \epsilon N$, where $\epsilon = 1$ or -1. We have $\epsilon = -1$ for either p and q satisfying (2) and n even or p and q satisfy (3) with n odd. Otherwise $\epsilon = 1$.

Proof. First suppose p and q satisfy (2). Thus $p = aP_{n+2} - bP_{n+1}$ and

$$q = aP_{n+1} - bP_n = -bP_{n+2} + (a+2b)P_{n+1}.$$

Hence,

$$p^2 - q^2 - 2pq = (a^2 + 2ab - b^2)(P_{n+2}^2 - 2P_{n+2}P_{n+1} - P_{n+1}^2) = N(-1)^{n+1} = \epsilon N,$$

where $\epsilon = -1$ for n even and $\epsilon = 1$ for n odd. Now we shall show that $p \geqslant q \geqslant 0$. Since $n \geqslant 0$,

$$P_{n+2} - P_{n+1} = P_{n+1} + P_n \geqslant P_{n+1} - P_n.$$

Therefore, since $a \geqslant b$,

$$aP_{n+2} - aP_{n+1} \geqslant bP_{n+1} - bP_n.$$

This implies $p \geqslant q$. Since $a \geqslant b$ and, for $n \geqslant 0$, $P_{n+1} \geqslant P_n$, we see that $aP_{n+1} \geqslant bP_n$ and this implies $q \geqslant 0$.

If p and q satisfy (3) then

$$p^2 - q^2 - 2pq = N(-1)^{n+2} = \epsilon N,$$

where $\epsilon = -1$ for n odd and $\epsilon = 1$ for n even. Since $n \geqslant 0$, $P_{n+2} \geqslant P_{n+1}$ and $P_{n+1} \geqslant P_n$. Hence

$$p = bP_{n+2} + aP_{n+1} \geqslant bP_{n+1} + aP_n = q.$$

Since $a \geqslant 0$, $b \geqslant 0$, $P_{n+1} > 0$, and $P_n \geqslant 0$, $q = bP_{n+1} + aP_n > 0$.

REFERENCES

1. Ernst M. Cohn, "Pell Number Triples," *The Fibonacci Quarterly,* Vol. 10, No. 2 (Oct. 1972), pp. 403–404 and 412.
2. Trygve Nagell, *Introduction to Number Theory,* Chelsea, 1964.

****