On the Pell Equation $x^2 - (k^2 - 2)y^2 = 2^t$

Ahmet Tekcan

1 Introduction.

Let $d \neq 1$ be a positive non-square integer and N be any fixed positive integer. Then the equation

$$x^2 - dy^2 \;=\; \pm N \qquad (1.1)$$

is known as "Pell's equation" after John Pell (1611-1685), who searched for integer solutions to equations of this type. Ironically, Pell was not the first to work on this problem, nor did he contribute to our knowledge for solving it. Euler (1707-1783), who brought us the ϕ-function, named the equation after Pell, and the name stuck.

For $N = 1$, the Pell equation

$$x^2 - dy^2 \;=\; \pm 1 \qquad (1.2)$$

is known as the *classical* Pell equation. Its complete theory was worked out by Lagrange (1736-1813), not Pell. It is often said that Euler mistakenly attributed Brouncker's (1620-1684) work on this equation to Pell. However, the equation appears in a book by Rahn (1622-1676), which was certainly written with Pell's help. Perhaps Euler knew what he was doing in naming the equation. Further details can be found in [2], [6], and [7].

In this article, we will define by recurrence an infinite sequence of positive solutions of the Pell equation $x^2 - dy^2 = 2^t$, where $d = k^2 - 2$ with $k > 2$ an integer and $t \geq 0$ is also an integer. We will also express these solutions using matrices that depend only on k and t.

2 Preliminary facts.

The Pell equation in (1.2) has infinitely many integer solutions. The first non-trivial positive integer solution (x_1, y_1) (first in the sense that x_1 or $x_1 + y_1\sqrt{d}$ is minimal) is called the *fundamental solution*, because it generates all the other solutions. In fact, if (x_1, y_1) is the fundamental solution of $x^2 - dy^2 = 1$, then the n^{th} positive solution (x_n, y_n) is defined by

$$x_n + y_n\sqrt{d} \;=\; (x_1 + y_1\sqrt{d})^n \qquad (2.1)$$

for any integer $n \geq 2$. (Furthermore, all non-trivial solutions can be obtained by considering the four cases $(\pm x_n, \pm y_n)$ for $n \geq 1$.)

There are several methods for finding the fundamental solution of Pell's equation $x^2 - dy^2 = 1$ for a positive non-square integer d. For example, the cyclic method known in India in the 12$^{\text{th}}$ century, and the slightly less efficient but more regular English method (17$^{\text{th}}$ century) produce all solutions of $x^2 - dy^2 = 1$ (see [3, pp. 30, 32]). But the most efficient method for finding the fundamental solution is based on the simple finite continued fraction expansion of $\sqrt{d}$. We can describe it as follows (see [1] and [4, p. 154]).

Let $[a_0; \overline{a_1, \ldots, a_r, 2a_0}\,]$ be the simple continued fraction expansion of $\sqrt{d}$ ($a_0 = \lfloor \sqrt{d} \rfloor$). Let $p_0 = a_0$, $p_1 = 1 + a_0 a_1$, $q_0 = 1$, $q_1 = a_1$, and

$$\begin{cases} p_n = a_n p_{n-1} + p_{n-2}\,, \\ q_n = a_n q_{n-1} + q_{n-2}\,, \end{cases} \qquad \text{for } n \geq 2.$$

If r is odd, the fundamental solution is $(x_1, y_1) = (p_r, q_r)$, where p_r/q_r is the r^{th} convergent of $\sqrt{d}$; if r is even, the fundamental solution is $(x_1, y_1) = (p_{2r+1}, q_{2r+1})$.

In connection with (1.1), it is well known ([6, Theorem 8.8, p. 146]) that if (u_1, v_1) is a solution of (1.1) and (x_1, y_1) is a solution of $x^2 - dy^2 = 1$, then (u, v) is a solution of (1.1), where

$$u + dv = (x_1 + dy_1)(u_1 + dv_1)\,. \tag{2.2}$$

However, in general ([6, p. 146, example below Theorem 8.8]), for $N \neq 1$ there is no a fundamental solution of $x^2 - dy^2 = \pm N$ (that is, a positive solution (u_1, v_1) such that for any positive solution (u, v), we have $(u, v) = (u_n, v_n)$ for some $n \in \mathbb{N}$). A general procedure to obtain the positive solutions of a solvable Pell equation $x^2 - dy^2 = N$ (for $N > 1$) can be found in [6, pp. 147–148, Theorem 8.9].

3 The Pell equation $x^2 - (k^2 - 2)y^2 = 2^t$.

First we consider the case $t = 0$; that is, the classical equation $x^2 - (k^2 - 2)y^2 = 1$.

Theorem 1 Let $d = k^2 - 2$ with $k \geq 2$.

(a) The continued fraction expansion of $\sqrt{d}$ is given by

$$\sqrt{d} = \begin{cases} [1; \overline{2}\,] & \text{if } k = 2\,, \\ [k-1; \overline{1, k-2, 1, 2k-2}\,] & \text{otherwise.} \end{cases} \tag{3.1}$$

(b) The fundamental solution of $x^2 - dy^2 = 1$ is

$$(x_1, y_1) = (k^2 - 1, k)\,. \tag{3.2}$$

Proof: (a) The case $k = 2$ can be easily verified. Suppose that $k \geq 3$. Then (3.1) follows, because

$$\begin{aligned}
\sqrt{k^2-2} &= k-1+\left(\sqrt{k^2-2}-(k-1)\right) = k-1+\cfrac{1}{\cfrac{1}{\sqrt{k^2-2}-(k-1)}} \\
&= k-1+\cfrac{1}{1+\cfrac{1}{\cfrac{\sqrt{k^2-2}+(k-2)}{2}}} = k-1+\cfrac{1}{1+\cfrac{1}{k-2+\cfrac{1}{\cfrac{2}{\sqrt{k^2-2}-(k-2)}}}} \\
&= k-1+\cfrac{1}{1+\cfrac{1}{k-2+\cfrac{1}{1+\cfrac{\sqrt{k^2-2}-(k-1)}{2k-3}}}} \\
&= k-1+\cfrac{1}{1+\cfrac{1}{k-2+\cfrac{1}{1+\cfrac{1}{\sqrt{k^2-2}+(k-1)}}}} \\
&= k-1+\cfrac{1}{1+\cfrac{1}{k-2+\cfrac{1}{1+\cfrac{1}{2k-2+\left(\sqrt{k^2-2}-(k-1)\right)}}}}.
\end{aligned}$$

(b) The case $k = 2$ of (3.2) follows because $(x, y) = (3, 2)$ is clearly a minimum solution. On the other hand, using the method from part (a) above, for $k \geq 3$ we have $r = 3$, $a_0 = k-1$, $a_1 = 1$, $a_2 = k-2$, $a_3 = 1$. Hence, $p_0 = k-1$, $p_1 = k$, $p_2 = k^2-k-1$, $p_3 = k^2-1$, $q_1 = 1$, $q_2 = k-1$, and $q_3 = k$. Thus, $(x_1, y_1) = (p_3, q_3) = (k^2-1, k)$. ∎

Next we consider the general case.

Theorem 2 Let k, t, d be arbitrary integers with $k \geq 2$, $t \geq 0$, and $d = k^2 - 2$. Define a sequence $\{(u_n, v_n)\}$ of positive integers by

$$(u_1, v_1) = \begin{cases} \left(2^{(t-1)/2}k, 2^{(t-1)/2}\right) & \text{if } t \text{ is odd}, \\ \left(2^{t/2}(k^2-1), 2^{t/2}k\right) & \text{if } t \text{ is even}. \end{cases} \tag{3.3}$$

and, for $n \geq 2$,

$$(u_n, v_n) = \left(u_1 x_{n-1} + d v_1 y_{n-1}, v_1 x_{n-1} + u_1 y_{n-1}\right), \tag{3.4}$$

where $\{(x_n, y_n)\}$ is the sequence of positive solutions of $x^2 - dy^2 = 1$. Then

(a) (u_n, v_n) is a solution of $x^2 - dy^2 = 2^t$ for any integer $n \geq 1$.

(b) For $n \geq 1$, we have

$$\begin{cases} u_{n+1} = (k^2-1)u_n + (k^3-2k)v_n, \\ v_{n+1} = ku_n + (k^2-1)v_n. \end{cases} \tag{3.5}$$

(c) For $n \geq 1$, we have

$$\begin{pmatrix} u_n \\ v_n \end{pmatrix} = \begin{cases} 2^{(t-1)/2} \begin{pmatrix} k^2-1 & k^3-2k \\ k & k^2-1 \end{pmatrix}^{n-1} \begin{pmatrix} k \\ 1 \end{pmatrix} & \text{if } t \text{ is odd,} \\ 2^{t/2} \begin{pmatrix} k^2-1 & k^3-2k \\ k & k^2-1 \end{pmatrix}^{n} \begin{pmatrix} 1 \\ 0 \end{pmatrix} & \text{if } t \text{ is even.} \end{cases} \tag{3.6}$$

Proof: (a) Assume t is odd. We have that $(u_1, v_1) = \left(2^{(t-1)/2}k, 2^{(t-1)/2}\right)$ is a solution of $x^2 - dy^2 = 2^t$, because

$$\begin{aligned} u_1^2 - dv_1^2 &= \left(2^{(t-1)/2}k\right)^2 - (k^2-2)\left(2^{(t-1)/2}\right)^2 \\ &= 2^{t-1}k^2 - 2^{t-1}k^2 + 2 \cdot 2^{t-1} = 2^t \,. \end{aligned}$$

Similarly it can be shown that $(u_1, v_1) = \left(2^{t/2}(k^2-1), 2^{t/2}k\right)$ is a solution when t is even.

On the other hand, rewriting (3.4) as

$$u_n + v_n\sqrt{d} = (x_{n-1} + y_{n-1}\sqrt{d})(u_1 + v_1\sqrt{d}) \,, \tag{3.7}$$

we see from (2.2) that (u_n, v_n) is also a solution for each $n \geq 2$. This can also be proved directly as follows:

$$\begin{aligned} u_n^2 - dv_n^2 &= (u_1x_{n-1} + dv_1y_{n-1})^2 - d(v_1x_{n-1} + u_1y_{n-1})^2 \\ &= u_1^2(x_{n-1}^2 - dy_{n-1}^2) - dv_1^2(x_{n-1}^2 - dy_{n-1}^2) \\ &= (x_{n-1}^2 - dy_{n-1}^2)(u_1^2 - dv_1^2) = 2^t \,. \end{aligned}$$

(b) Using repeatedly (2.1) and (3.7), we obtain

$$\begin{aligned} u_{n+1} + v_{n+1}\sqrt{d} &= (x_n + y_n\sqrt{d})(u_1 + v_1\sqrt{d}) \\ &= (x_1 + y_1\sqrt{d})^n(u_1 + v_1\sqrt{d}) \\ &= (x_1 + y_1\sqrt{d})\left[(x_1 + y_1\sqrt{d})^{n-1}(u_1 + v_1\sqrt{d})\right] \\ &= (x_1 + y_1\sqrt{d})\left[(x_{n-1} + y_{n-1}\sqrt{d})(u_1 + v_1\sqrt{d})\right] \\ &= (x_1 + y_1\sqrt{d})(u_n + v_n\sqrt{d}) \,, \end{aligned}$$

which is equivalent to (3.5).

(c) We can rewrite (3.5) in the form $\begin{pmatrix} u_{n+1} \\ v_{n+1} \end{pmatrix} = \begin{pmatrix} x_1 & dy_1 \\ y_1 & x_1 \end{pmatrix} \begin{pmatrix} u_n \\ v_n \end{pmatrix}$. Hence, proceeding by induction on $n \geq 1$, we obtain

$$\begin{pmatrix} u_n \\ v_n \end{pmatrix} = \begin{pmatrix} x_1 & dy_1 \\ y_1 & x_1 \end{pmatrix}^{n-1} \begin{pmatrix} u_1 \\ v_1 \end{pmatrix} .$$

Now (3.6) follows from (3.3), because

$$\begin{pmatrix} k^2-1 \\ k \end{pmatrix} = \begin{pmatrix} x_1 & dy_1 \\ y_1 & x_1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} .$$

■

Example 3.1 Let $k = 4$. Then the fundamental solution of $x^2 - 14y^2 = 1$ is $(x_1, y_1) = (15, 4)$, and some other solutions are

$$(x_2, y_2) = (449, 120), \quad (x_3, y_3) = (13455, 3596),$$
$$(x_4, y_4) = (403201, 107760), \quad (x_5, y_5) = (12082575, 3229204),$$
$$\text{and} \quad (x_6, y_6) = (362074049, 96768360).$$

Let $t = 6$. A solution of $x^2 - 14y^2 = 64$ is given by $(u_1, v_1) = (120, 32)$. Hence, using (3.5), we get

$$(u_2, v_2) = (3592, 960), \quad (u_3, v_3) = (107640, 28768),$$
$$(u_4, v_4) = (3225608, 862080), \quad (u_5, v_5) = (96660600, 25833632),$$
$$(u_6, v_6) = (2896592392, 774146880).$$

Problem. Prove or disprove that (u_1, v_1) is a fundamental solution of

$$x^2 - (k^2 - 2)y^2 = 2^t \quad (\text{for } t \geq 1).$$

References

[1] Baltus, C., Continued Fractions and the Pell Equations: The work of Euler and Lagrange, *Comm. Anal. Theory Contin. Fractions*, **3**(1994), 4–31.

[2] Barbeau, E., *Pell's Equation*, Springer Verlag, 2003.

[3] Edwards, H.M., *Fermat's Last Theorem: A Genetic Introduction to Algebraic Number Theory*, Corrected reprint of the 1977 original, Graduate Texts in Mathematics, 50, Springer Verlag, New York, 1996.

[4] Koblitz, N., *A Course in Number Theory and Cryptography*, Graduate Texts in Mathematics, Second Edition, Springer Verlag, 1994.

[5] Lenstra, H.W., Solving The Pell Equation, *Notices of the AMS*, **49**(2) (2002), 182–192.

[6] Leveque, W.J., *Topics in Number Theory*, Volume 1, Dover Publications, 2002.

[7] Niven I., Zuckerman, H.S., and Montgomery, H.L., *An Introduction to the Theory of Numbers*, Fifth Edition, John Wiley & Sons, Inc., New York, 1991.

Ahmet Tekcan
Uludag University
Faculty of Science
Department of Mathematics
Görükle 16059
Bursa-TURKEY
tekcan@uludag.edu.tr
http://matematik.uludag.edu.tr/AhmetTekcan.htm