APPLICATION TO PELL'S EQUATIONS

Nabikhonov Nabikhon Yokubjon ugli
Student of the National University of Uzbekistan, winner of the International Olympiads
Nabikhonov Akbarkhon Yokubkhon ugli
Student of Gulistan State University, winner of the Republican Olympiads

Annotation: *This article reflects on the* ***Pell's equations****, one of the* ***Diophantine equations*** *(i.e. equations requiring a solution in integers). All solutions to this equation have been found and an overview is given. The general solution to the* ***Pell's equation*** *using matrices is an easy-to-define method. The application of the* ***Pell's equations*** *has been described. Solutions to complex Olympic problems are given. At the end of the article, enough problems are given to work independently.*

Keywords*:* ***Pell's equation,*** *perfect square, Hilbert's 10th problem, fundamental solution,* ***matrix of the Pell's equation****, multiplication principle, sequence, recursive system, eigenvalues, characteristic equation, Pell resolvent equation, prime numbers, positive integer numbers.*

1. INTRODUCTION

Pell's equation has an exceptional history, described in detail in [6, 8]. Firstly, John Pell (1611–1685) has nothing to do with the equation, except the fact that Leonhard Euler (1707–1783) mistakenly attributed to Pell a solution method founded by William Brouncker (1620–1684). Solutions of Pell's equation for special cases (e.g., $D = 2$) were even considered in India and Greece around 400 BC. The first description of a method which allowed to construct a nontrivial solution of the equation for an arbitrary D can be found, e.g. in Euler's Algebra, but the method was described without any justification guaranteeing that it would find at least one solution. The first proof of correctness was published by Joseph Louis Lagrange [9].

Let $D > 1$ be an integer which is not a perfect square. The diophantine equation, called ***Pell's equation (alternatively called the Pell-Fermat equation)***:

$$x^2 - Dy^2 = 1 \qquad (1.1)$$

has an obviously solution $(1,0)$ in nonnegative integers. If D is perfect square, then given equation has only one solution, that $(1,0)$. Really, if assume that $D = d^2$, then since (1.1), we have follow equation:

$$(x - dy)(x + dy) = 1.$$

Hence $x = 1$ and $y = 0$.

A well-known but nontrivial result (which we take for granted) is that this equation also has nontrivial solutions (i.e., different from $(1,0)$). In this article we explain how the theory developed so far allows finding all solutions of the Pell equation once we know the smallest nontrivial solution.

Definition 1.1. Let S_D be the set of all solutions in positive integers to the Eq.(1.1). Let (x_1, y_1) called the fundamental solution, if the solution in S_D for which the first component x_1 is minimal among the first components of the elements of S_D.

Theorem 1.1. The ***Pell's equation*** always has a solution (x, y).

We have given the proof of this theorem above. In fact, there are infinitely many solutions to the equation! Given that there is one solution, we can generate more from it.

The Pell equation has been widely used in solving many problems in mathematics. From our point of view, the most significant application of Pell's equation was done in the proof of Matiyasevich's theorem [4] that we try to formalize in the Mizar system [3]. That theorem states that every computable enumerable set is diophantine. It implies the undecidability of Hilbert's 10th problem. The proof is based mainly on a particular case

$$x^2 - (a^2 - 1)y^2 = 1$$

where a is a natural number.

2. Matrix of the *Pell's equation.*

Our main goal is to find all solutions to the equation of a given Pell. First we need to define somethings.

Definition 2.1. If x, y are positive integers, consider the matrix

$$A_{(x,y)} = \begin{bmatrix} x & Dy \\ y & x \end{bmatrix}$$

This matrix called **matrix of the *Pell's equation.***

Obviously, $(x, y) \in S_D$ if and only if $\det A_{(x,y)} = 1$.

Lemma 2.1. For matrix $A_{(x,y)}$, the following holds

$$A_{(x,y)} \cdot A_{(u,v)} = A_{(xu+Dyv,xv+yu)}.$$

Proof: By elementary computations we obtain the proof:

$$A_{(x,y)} \cdot A_{(u,v)} = \begin{bmatrix} x & Dy \\ y & x \end{bmatrix} \cdot \begin{bmatrix} u & Dv \\ v & u \end{bmatrix} = \begin{bmatrix} xu + Dyv & D(xv + yu) \\ xv + yu & xu + Dyv \end{bmatrix} == A_{(xu+Dyv,xv+yu)}$$

Passing to determinants in **Lemma 2.1** we obtain the **multiplication principle:** if $(x, y), (u, v) \in S_D$, then $(xu + Dyv, xv + yu) \in S_D$.

It follows from the multiplication principle that if we write

$$A^n_{(x_1,y_1)} = \begin{bmatrix} x_n & Dy_n \\ y_n & x_n \end{bmatrix}, \quad n \geq 1.$$

then $(x_n, y_n) \in S_D$ for all n. The sequences x_n and y_n are described by the recursive system

$$\begin{cases} x_{n+1} = x_1 x_n + D y_1 y_n \\ y_{n+1} = y_1 x_n + y_n x_1, \end{cases} \quad n \geq 1 \qquad (2.1)$$

consequence of the equality $A^{n+1}_{(x_1,y_1)} = A_{(x_1,y_1)} A^n_{(x_1,y_1)}$.

We give the theorem about the Matrix and its eigenvalues. We use this theorem to find solutions to the Eq.(1.1). This theorem is considered important in matrix theory (see [1]).

Theorem 2.1. Let $A \in M_2(\mathbb{C})$ and let λ_1, λ_2 be its eigenvalues.

(a) If $\lambda_1 \neq \lambda_2$, then for all $n \geq 1$ we have $A^n = \lambda_1^n B + \lambda_2^n C$, where $B = \frac{1}{\lambda_1 - \lambda_2}(A - \lambda_2 I_2)$ and $C = \frac{1}{\lambda_2 - \lambda_1}(A - \lambda_1 I_2)$.

(b) If $\lambda_1 = \lambda_2$, then for all $n \geq 1$ we have $A^n = \lambda_1^n B + n\lambda_1^{n-1} C$, where $B = I_2$ and $C = A - \lambda_1 I_2$.

3. Solution of the *Pell's equation.*

Theorem 2.1 gives explicit formula for x_n and y_n in terms of x_1, y_1, n: the characteristic equation of matrix $A_{(x_1,y_1)}$ is

$$\lambda^2 - 2x_1\lambda + 1 = 0$$

with $\lambda_{1,2} = x_1 + \sqrt{x_1^2 - 1} = x_1 \pm y_1\sqrt{D}$, and **Theorem 2.1** yields, after an elementary computation of the matrices B, C involved in that theorem

$$\begin{cases} x_n = \frac{1}{2}\left[(x_1 + y_1\sqrt{D})^n + [(x_1 - y_1\sqrt{D})^n\right] \\ y_n = \frac{1}{2\sqrt{D}}\left[(x_1 + y_1\sqrt{D})^n + [(x_1 - y_1\sqrt{D})^n\right] \end{cases} n \geq 1. \qquad (3.1)$$

If $n = 0$, in which case it gives the trivial solution $(x_0, y_0) = (1,0)$.

Theorem 3.1. All solutions in positive integers of the ***Pell's equation*** $\mathrm{x}^2 - \mathrm{D}\mathrm{y}^2 = 1$ are described by the formula (3.1), where $(\mathrm{x}_1, \mathrm{y}_1)$ is the fundamental solution of the equation.

Proof: Suppose that there are elements in S_D which are not covered by formula (3.1), and among them choose one (x, y) for which x is minimal. Using the multiplication principle, we observe that the matrix $A_{(x,y)}\ A^{-1}_{(x_1,y_1)}$ generates a solution in integers (x', y'), where

$$\begin{cases} x' = x_1 x - D y_1 y \\ y' = -y_1 x + x_1 y \end{cases}$$

We claim that x', y' are positive integers. This is clear for x', as $x > \sqrt{D}y$ and $x_1 > \sqrt{D}y_1$, thus $x_1 x > D y_1 y$. Also, $x_1 y > y_1 x$ is equivalent to $x_1^2(x^2 - 1) > x^2(x_1^2 - 1)$ or $x > x_1$, which holds because (x_1, y_1) is a fundamental solution and $(x, y)$is not described by relation (3.1) (while (x_1, y_1) is described by this relation, with $n = 1$). Moreover, since $A_{(x',y')}A_{(x_1,y_1)} = A_{(x,y)}$, we have $x = x'x_1 + Dy'y_1 > x'$ and $y = x'y_1 + y'x_1 > y'$. By minimality, (x', y') must be of the form (3.1), i.e., $A_{(x,y)}A^{-1}_{(x_1,y_1)} = A^k_{(x_1,y_1)}$ for some positive integer k. Therefore $A_{(x,y)} = A^{k+1}_{(x_1,y_1)}$, i.e., (x, y) is of the form (3.1), a contradiction.

Example 3.1. Find all solutions in positive integers to Pell's equation

$$x^2 - 2y^2 = 1.$$

Solution: The fundamental solution is $(x_1, y_1) = (3,2)$ and the associated matrix is

$$A_{(3,2)} = \begin{bmatrix} 3 & 4 \\ 2 & 3 \end{bmatrix}$$

The solutions $(x_n, y_n)_{n\geq 1}$ are given by $A^n_{(3,2)}$, i.e.

$$\begin{cases} x_n = \frac{1}{2}\left[\left(3+2\sqrt{2}\right)^n + \left(3-2\sqrt{2}\right)^n\right] \\ y_n = \frac{1}{2\sqrt{2}}\left[\left(3+2\sqrt{2}\right)^n - \left(3-2\sqrt{2}\right)^n\right]. \end{cases}$$

We can extend slightly the study of the Pell equation by considering the more general equation

$$ax^2 - by^2 = 1 \qquad (3.2)$$

where we assume that ab is not a perfect square (it is not difficult to see that if ab is a square, then the equation has only trivial solutions). Contrary to the Pell equation, this Eq. (3.2) does not always have solutions (the reader can check that the equation $3x^2 - y^2 = 1$ has no solutions in integers by working modulo 3).

Define the **Pell resolvent** of (3.2) by

$$u^2 - abv^2 = 1 \qquad (3.3)$$

and let $S_{a,b}$ be the set of solutions in positive integers of Eq.(3.2). Thus $S_{1,ab}$ is the set denoted S_{ab} when considering the Pell equation (it is the set of solutions of the Pell resolvent). If x, y, u, v are positive integers consider the matrices

$$B_{(x,y)} = \begin{bmatrix} x & by \\ y & ax \end{bmatrix}, \qquad A_{(u,v)} = \begin{bmatrix} u & abv \\ v & u \end{bmatrix},$$

the second matrix being the matrix associated with the Pell resolvent equation.

By the computations as above, we obtain:

if $(x, y) \in S_{a,b}$ and $(u, v) \in S_{ab}$, then $(xu + byv, axv + yu) \in S_{a,b}$,

Using the previous theorem and the multiplication principle, one easily obtains the following result, whose formal proof is left to the reader.

Theorem 3.2. Assume that Eq. (3.2) is solvable in positive integers, and let (x_0, y_0) be its minimal solution (i.e., x_0 is minimal). Let (u_1, v_1) be the fundamental solution of the resolvent Pell equation (3.5). Then all solutions (x_n, y_n) in positive integers of Eq. (3.2) are generated by

$$B_{(x_n,y_n)} = B_{(x_0,y_0)} A_{(u_1,v_1)}, \quad n \geq 0 \qquad (3.4)$$

It follows easily from (3.4) that

$$\begin{cases} x_n = x_0 u_n + b y_0 v_n \\ y_n = y_0 u_n + a x_0 v_n \end{cases} \quad n \geq 0 \qquad (3.5)$$

where $(u_n, v_n)_{n\geq 1}$ is the general solution to the Pell resolvent equation.

Below we will consider the problems with the application of the Pell equation.

4. Application of the *Pell's Equations.*

4.1. Examples.

Example 4.1.1. Solve in positive integers the equation

$$6x^2 - 5y^2 = 1.$$

Solution: This equation is solvable and its minimal solution is $(x_0, y_0) = (1,1)$. The Pell resolvent equation is $u^2 - 30v^2 = 1$, with fundamental solution $(u_1, v_1) = (11, 2)$. Using formula (3.5) and then (3.1), we deduce that the solutions in positive integers are$(x_n, y_n)_{n\geq 1}$, where

$$\begin{cases} x_n = \frac{6+\sqrt{30}}{12}\left(11+2\sqrt{30}\right)^n + \frac{6-\sqrt{30}}{12}\left(11-2\sqrt{30}\right)^n \\ y_n = \frac{5+\sqrt{30}}{12}\left(11+2\sqrt{30}\right)^n + \frac{5-\sqrt{30}}{12}\left(11-2\sqrt{30}\right)^n. \end{cases}$$

Example 4.1.2 (Kursak Competition). Prove that if $m = 2 + 2\sqrt{28n^2+1}$ is an integer for some $n \in \mathbb{N}$, then m is a perfect square.

Proof: For m to be an integer, we must have $28n^2 + 1 = x^2$ for some x. This is Pell's equation with $D = 28$. If we try to find the fundamental solution, we have a really hard time doing so. Hence we adopt a trick: write the equation as $x^2 - 7(2n)^2 = 1$.

The fundamental solution to $X^2 - 7Y^2 = 1$ is not hard to find, and it is $(8, 3)$. Here, 3 is odd. We generate more solutions from this till we find the second number even.

$$\left(8+3\sqrt{7}\right)^2 = 127 + 48\sqrt{7}.$$

Thus $(127, 24)$ is the fundamental solution to $x^2 - 28n^2 = 1$. (Because $127 + 48\sqrt{7} = 127 + 24\sqrt{28}$)Since (3.1), we have:

$$x_k = \frac{1}{2}\left[\left(127+24\sqrt{28}\right)^k + \left(127-24\sqrt{28}\right)^k\right]$$

Therefore,

$$2x + 2 = \left(127+24\sqrt{28}\right)^k + \left(127-24\sqrt{28}\right)^k + 2 =$$
$$= \left(8+3\sqrt{7}\right)^{2k} + \left(8-3\sqrt{7}\right)^{2k} + 2\left(8+3\sqrt{7}\right)^k\left(8-3\sqrt{7}\right)^k =$$
$$= \left[\left(8+3\sqrt{7}\right)^k + \left(8-3\sqrt{7}\right)^k\right]^2$$

and we are done!

Example 4.1.3. (Vietnam 2016). Find all n such that

$$\sqrt{\frac{7^n+1}{2}}$$

is a prime.

Solution: Suppose this equals p. Squaring and rearranging, we find $2p^2 - 7^n = 1$. This is not Pell's equation if n is odd. We can easily see that $n = 1$ works. So when $n > 1$ small cases suggest that n odd doesn't seem to work. This observation is correct; modulo 8; the equation implies n is even. So we have the negative Pell's equation:

$$2p^2 - (7^m)^2 = 1$$

where $m = \frac{n}{2}$. So consider the general Pell's equation $2y^2 - x^2 = 1$. Since $(1, 1)$ is a solution, hence the general solution for x_n is

$$x_{n-1} = \frac{1}{2}\left[\left(1+\sqrt{2}\right)^{2k+1} + \left(1-\sqrt{2}\right)^{2k+1}\right] =$$

$$= \frac{1+\sqrt{2}}{2}\left(3+2\sqrt{2}\right)^k + \frac{1-\sqrt{2}}{2}\left(3-2\sqrt{2}\right)^k$$

So we obtain the recurrence $x_n = 6x_{n-1} - x_{n-2}$ with $(x_0, x_1) = (1, 7)$. Similarly we get $y_n = 6y_{n-1} - y_{n-2}$ with $(y_0, y_1) = (1, 5)$. Then

$x_n \equiv -(x_{n-1} + x_{n-2}) \pmod 7$, $\quad y_n \equiv y_{n-1} - y_{n-2} \pmod 5$.

Hence, $7 | x_n$ if and only if $n \equiv 1 \pmod 3$, which also corresponds to $5 | y_n$. Hence, we must have $p = 5$ and so the only other solution we get is $n = 2$.

4.2. Problems for Practice.

Problem 4.2.1. A triangular number is a number of the form

$$1 + 2 + \cdots + n$$

for some positive integer n. Find all triangular numbers which are perfect squares.

Problem 4.2.2. Find all positive integers n such that $n+1$ and $3n+1$ are simultaneously perfect squares.

Problem 4.2.3. Find all integers a, b such that

$a^2 + b^2 = 1 + 4ab$.

Problem 4.2.4. The difference of two consecutive cubes equals n^2 for some positive integer n. Prove that $2n - 1$ is a perfect square.

Problem 4.2.5. Find all triangles whose side lengths are consecutive integers and whose area is an integer.

REFERENCES :

[1] Titu Andreescu, Essential Linear Algebra with Applications, A Problem-Solving Approach, Springer Science+Business Media New York, 2014.

[2] Aditya Khurmi, Modern Olympiad Number Theory, 2020.

[3] Grzegorz Bancerek, Czeslaw Byliński, Adam Grabowski, Artur Korniłowicz, Roman Matuszewski, Adam Naumowicz, Karol Pąk, and Josef Urban. Mizar: State-of-the-art and beyond. Intelligent Computer Mathematics, volume 9150 of Lecture Notes in Computer Science, pages 261–279. Springer International Publishing, 2015.

[4] Yuri Matiyasevich. Martin Davis and Hilbert's Tenth Problem. Martin Davis on Computability, Computational Logic and Mathematical Foundations, pages 35–54, 2017.

[5] Waclaw Sierpiński. Elementary Theory of Numbers. PWN, Warsaw, 1964.

[6] Andre Weil. Number Theory. An Approach through History from Hammurapi to Legendre. Birkhauser, Boston, Mass., 1983.

[7] Titu Andreescu, Gabriel Dospinescu, Oleg Mushkarov, NUMBER THEORY: CONCEPTS AND PROBLEMS, XYZ Press, LLC-2017.

[8] Hendrik W. Lenstra. Solving the Pell equation. Algorithmic Number Theory, 44:1–24, 2008.

[9] Joseph L. Lagrange. Solution d'un proble`eme d'arithm´ etique. Me´langes de philosophie et de math. de la Socie´te´ Royale de Turin, (44–97), 1773.

[10] www.aops.com internet sayti.

[11] https://math.stackexchange.com/ internet sayti.

[12] http://www.imo-official.org/ internet sayti.