The IMO Compendium Group
Olympiad Training Materials
www.imomath.com

Pell's Equation

Dušan Djukić

Contents

1 Introduction

Definition 1. Pell's equation *is a diophantine equation of the form* $x^2 - dy^2 = 1$, $x, y \in \mathbb{Z}$, *where* d *is a given natural number which is not a square.*

An equation of the form $x^2 - dy^2 = a$ *for an integer* a *is usually referred to as a* Pell-type equation.

An arbitrary quadratic diophantine equation with two unknowns can be reduced to a Pell-type equation. How can such equations be solved? Recall that the general solution of a linear diophantine equation is a linear function of some parameters. This does not happen with general quadratic diophantine equations. However, as we will see later, in the case of such equations with two unknowns there still is a relatively simple formula describing the general solution.

Why does the definition of Pell's equations assume d is not a square? Well, for $d = c^2$, $c \in \mathbb{Z}$, the equation $x^2 - dy^2 = a$ can be factored as $(x - cy)(x + cy) = a$ and therefore solved without using any further theory. So, unless noted otherwise, d will always be assumed not to be a square.

The equation $x^2 - dy^2 = a$ can still be factored as

$$(x + y\sqrt{d})(x - y\sqrt{d}) = a.$$

In order to be able to make use of this factorization, we must deal with numbers of the form $x + y\sqrt{d}$, where x, y are integers. This set is denoted by $\mathbb{Z}[\sqrt{d}]$. An important property of this set is that the sum and product of two of its elements remain in the set (i.e. this set is really a ring).

Definition 2. *The* conjugate *of number* $z = x + y\sqrt{d}$ *is defined as* $\overline{z} = x - y\sqrt{d}$, *and its* norm *as* $N(z) = z\overline{z} = x^2 - dy^2 \in \mathbb{Z}$.

Theorem 1. *The norm and the conjugate are multiplicative in z:* $N(z_1 z_2) = N(z_1)N(z_2)$ *and* $\overline{z_1 z_2} = \overline{z_1} \cdot \overline{z_2}$.

Proof is straightforward. □

In terms of these concepts, equation $x^2 - dy^2 = a$ can be rewritten as

$$N(z) = a, \quad \text{where } z = x - y\sqrt{d} \in \mathbb{Z}[\sqrt{d}].$$

In particular, the Pell's equation becomes $N(z) = 1$, $z \in \mathbb{Z}[\sqrt{d}]$. We continue using these notation regularly.

Since z is a solution to a Pell-type equation if and only if so is $-z$, we always assume w.l.o.g. that $z > 0$.

Solutions of a Pell's Equation

A Pell's equation has one trivial solution, $(x,y) = (1,0)$, corresponding to solution $z = 1$ of equation $N(z) = 1$. But if we know the smallest *non-trivial* solution, then we can derive all the solutions. This is what the following statement claims.

Theorem 2. *If z_0 is the minimal element of $\mathbb{Z}[\sqrt{d}]$ with $z_0 > 1$ and $N(z_0) = 1$, then all the elements $z \in \mathbb{Z}[\sqrt{d}]$ with $Nz = 1$ are given by $z = \pm z_0^n$, $n \in \mathbb{Z}$.*

Proof. Suppose that $N(z) = 1$ for some $z > 0$. There is a unique integer k for which $z_0^k \le z < z_0^{k+1}$. Then the number $z_1 = zz_0^{-k} = z\overline{z_0}^k$ satisfies $1 \le z_1 < z_0$ and $N(z_1) = N(z)N(z_0)^{-k} = N(z) = 1$. It follows from the minimality of z_0 that $z_1 = 1$ and hence $z = z_0^k$. □

Corrolary. If (x_0, y_0) is the smallest solution of the Pell's equation with d given, then all natural solutions (x,y) of the equation are given by $x + y\sqrt{d} = \pm(x_0 + y_0\sqrt{d})^n$, $n \in \mathbb{N}$.

Note that $z = x + y\sqrt{d}$ determines x and y by the formulas $x = \frac{z+\overline{z}}{2}$ and $y = \frac{z-\overline{z}}{2\sqrt{d}}$. Thus all the solutions of the Pell's equation are given by the formulas

$$x = \frac{z_0^n + \overline{z_0}^n}{2} \quad \text{i} \quad y = \frac{z_0^n - \overline{z_0}^n}{2\sqrt{d}}.$$

Example 1. *The smallest non-trivial solution of the equation $x^2 - 2y^2 = 1$ is $(x,y) = (3,2)$. Therefore for every solution (x,y) there is an integer n such that $x + y\sqrt{d} = \pm(3 + 2\sqrt{2})^n$. Thus*

$$x = \frac{(3+2\sqrt{2})^n + (3-2\sqrt{2})^n}{2}, \quad y = \frac{(3+2\sqrt{2})^n - (3-2\sqrt{2})^n}{2\sqrt{2}}.$$

Now we will show that every Pell's equation indeed has a non-trivial solution.

Lemma 1 (Dirichlet's theorem). *Let α be an irrational number and n be a positive integer. There exist $p \in \mathbb{Z}$ and $q \in \{1,2,\dots,n\}$ such that $\left|\alpha - \frac{p}{q}\right| < \frac{1}{(n+1)q}$.*

Proof. The stated inequality is equivalent to $|q\alpha - p| < \frac{1}{n+1}$.

Let, as usual, $\{x\}$ denote the fractional part of real x. Among the $n+2$ numbers 0, $\{\alpha\}$, $\{2\alpha\}$, $\dots$, $\{n\alpha\}$, 1 in the segment $[0,1]$, some two will differ by less than $\frac{1}{n+1}$. If such are the numbers $\{k\alpha\}$ and $\{l\alpha\}$, it is enough to set $q = |k-l|$; and if such are $\{k\alpha\}$ and 0 or 1, it is enough to set $q = k$. In either case, p is the integer closest to $k\alpha$. □

Lemma 2. *If α is an arbitrary real number, then there exist infinitely many pairs of positive integers (p,q) satisfying $\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}$.*

Proof immediately follows from Dirichlet's theorem. □

Theorem 3. *A Pell's equation has a solution in the set of positive integers.*

Proof. Applying L.2 to $\alpha = \sqrt{d}$, we see that there exists an integer n with $|n| < 2\sqrt{d} + 1$ such that the equation $x^2 - dy^2 = n$ has infinitely many positive integral solutions (x,y). It follows that there are two different ones, say (x_1,y_1) i (x_2,y_2), that satisfy $x_1 \equiv x_2$ and $y_1 \equiv y_2 \pmod{n}$. Denote $z_1 = x_1 + y_1\sqrt{d}$ and $z_2 = x_2 + y_2\sqrt{d}$ and assume $z_1 > z_2$. Then $z_0 = z_1/z_2 > 1$ is an element of $\mathbb{Z}[\sqrt{d}]$ of norm 1 and corresponds to a non-trivial solution (x_0,y_0) of the Pell's equation. □

2 Pell-type Equations

A Pell-type equation in general may not have integer solutions (for example, the equation $x^2 - 3y^2 = 2$). When it does, it is possible to describe the general solution.

Theorem 4. *Equation $x^2 - dy^2 = -1$ has an integral solution if and only if there exists $z_1 \in \mathbb{Z}[\sqrt{d}]$ with $z_1^2 = z_0$.*

Proof. The "if" part is trivial. For the other direction we consider the smallest solution $z = z_1 \in \mathbb{Z}[\sqrt{d}]$ of the equation $N(z) = -1$ satisfying $z > 1$ and, like in theorem 2, deduce that $1 \le z_1 < z_0$. Since $z = z_1^2 < z_0^2$ is a solution of $N(z) = 1$, we must have $z_1^2 = z_0$. □

Consider the general equation $N(z) = a$. Like in the theorem 1, one can show that all its solutions can be obtained from the solutions z with $1 \le z \le z_0$, where z_0 is the smallest non-trivial solution of Pell's equation $N(z) = 1$. Thus it is always sufficient to check finitely many values of x. Moreover, there is a simple upper bound for those x.

Theorem 5. *If a is an integer such that the equation $N(z) = x^2 - dy^2 = a$ has an integer solution, then there is a solution with $|x| \le \dfrac{z_0+1}{2\sqrt{z_0}}\sqrt{|a|}$ and the corresponding upper bound for $y = \sqrt{\frac{x^2-a}{d}}$.*

Proof. If z_1 is a solution of the equation $N(z) = a$, then there is $m \in \mathbb{Z}$ for which $a/\sqrt{z_0} \le z_0^m z_1 < a\sqrt{z_0}$. Then $z_2 = z_0^m z_1 = x + y\sqrt{d}$ is a solution of the equation $N(z) = 1$ and satisfies

$$2|x| = \left| z_2 + \frac{a}{z_2} \right| \le \max_{[a/\sqrt{z_0}, a\sqrt{z_0})} \left| t + \frac{a}{t} \right| = \frac{z_0+1}{\sqrt{z_0}}\sqrt{|a|}. \ \square$$

Example 2. *Find all integer solutions of $x^2 - 7y^2 = 2$.*

Solution. The mimimal solution of the corresponding Pell's equation is $z_0 = 8 + 3\sqrt{7}$. We must find the solutions $z = x + y\sqrt{7}$ of $N(z) = 2$ satisfying $x \le \frac{z_0+1}{2\sqrt{z_0}}\sqrt{a} = 3$ and $y = \sqrt{\frac{x^2-2}{7}} \le 1$. The only such solution is $z = 3 + \sqrt{7}$. It follows that all solutions (x, y) of the given equation are given by

$$x + y\sqrt{7} = \pm(3+\sqrt{7})(8+3\sqrt{7})^n, \quad n \in \mathbb{N}. \ \triangle$$

3 Problems with Solutions

1. Solve in integers the equation $x^2 + y^2 - 1 = 4xy$.

   Solution. Substituting $u = y - 2x$ reduces the equation to $u^2 = 3x^2 + 1$ whose general solution is given by $x + u\sqrt{3} = (2+\sqrt{3})^n$.

2. For a given integer d, solve $x^2 - dy^2 = 1$ u skupu *racionalnih* brojeva.

   Solution. No knowledge of Pell's equation is required here. For $x \ne 1$ we have $d\left(\frac{y}{x-1}\right) = \frac{x+1}{y}$. Setting $\frac{y}{x-1} = t \in \mathbb{Q}$ we easily obtain $x = \frac{dt^2+1}{dt^2-1}$ i $y = \frac{2t}{dt^2-1}$.

3. Let $(x, y) = (a, b)$, $a, b \in \mathbb{N}$ be the smallest integer solution of $x^2 - dy^2 = 1$. Consider the sequence defined by $y_0 = 0$, $y_1 = b$, $y_{n+1} = 2ay_n - y_{n-1}$ for $n \ge 1$. Show that $ay_n^2 + 1$ is a square for each n. Show that if $ay^2 + 1$ is a square for some $y \in \mathbb{N}$, then $y = y_n$ for some n.

   Solution. Let $x_n + y_n' = \left(a + b\sqrt{d}\right)^n$. All solutions (x, y) of $x^2 = ay^2 + 1$ are given by $(x, y) = (x_n, y_n')$ for some n. We have

$$y_n' = \frac{1}{2\sqrt{d}}\left(\left(a+b\sqrt{d}\right)^n - \left(a-b\sqrt{d}\right)^n\right). \tag{1}$$

Since $a \pm b\sqrt{d}$ are the solutions of the quadratic equation $x^2 - 2ax + 1 = 0$, relation (1) easily implies that $y'_{n+2} - 2ay'_{n+1} + y_n = 0$. Therefore the sequences (y_n) and (y'_n) satisfy the same initial conditions and recurrent relation and must be equal. The statement of the problem follows immediately.

4. Prove that $5x^2 + 4$ or $5x^2 - 4$ is a perfect square if and only if x is a term in the Fibonacci sequence.

5. Find all $n \in \mathbb{N}$ such that $\binom{n}{k-1} = 2\binom{n}{k} + \binom{n}{k+1}$ for some natural number $k < n$.

   Solution. Multiplication by $\frac{(k+1)!(n-k+1)!}{n!}$ transforms the equation into $k(k+1) = 2(k+1)(n-k+1) + (n-k)(n-k+1)$, which is simplified as $n^2 + 3n + 2 = 2k^2 + 2k$, i.e.

   $$(2n+3)^2 + 1 = 2(2k+1)^2.$$

   The smallest solution of equation $x^2 - 2y^2 = -1$ is $(1,1)$, and therefore all its solutions (x_i, y_i) are given by $x_i + y_i\sqrt{2} = (1+\sqrt{2})^{2i+1}$. Note that x_i and y_i are always odd, so $n = \frac{x_i - 3}{2}$ is an integer and a solution to the problem. Clearly, there are no other solutions.

6. Let $a \in \mathbb{N}$ and $d = a^2 - 1$. If x, y are integers and the absolute value of $m = x^2 - dy^2$ is less than $2a + 2$, prove that $|m|$ is a perfect square.

   Solution. The smallest solution of $N(z) = 1$ is $z_0 = a + \sqrt{d}$. If $N(z) = m$ has a solution, then by the theorem 5 it also has a solution $z = x + y\sqrt{d}$ in which $x \le \frac{z_0+1}{2\sqrt{z_0}}\sqrt{|m|} = \sqrt{\frac{a+1}{2}|m|}$. For $|m| < 2a + 2$ this inequality becomes $x < a + 1$, and thus $(x,y) = (a,1)$ and $m = 1$ or $y = 0$ and $m = x^2$.

7. 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.

   Solution. We start by finding those n for which m is an integer. The pair $(\frac{m}{2} - 1, n)$ must be a solution of Pell's equation $x^2 - 28y^2 = 1$ whose smallest solution is $(x_0, y_0) = (127, 24)$; hence $\frac{m}{2} - 1 + n\sqrt{28} = (127 + 24\sqrt{28})^k$ for some $k \in \mathbb{N}$. Now we have

   $$m = 2 + (127 + 24\sqrt{28})^k + (127 - 24\sqrt{28})^k = A^2,$$

   where $A = (8 + 3\sqrt{7})^k + (8 - 3\sqrt{7})^k$ is an integer.

8. Prove that if the difference of two consecutive cubes is n^2, $n \in \mathbb{N}$, then $2n - 1$ is a square.

   Solution. Let $(m+1)^3 - m^3 = 3m^2 + 3m + 1 = n^2$. Then $(2n)^2 = 3(2m+1)^2 + 1$, so $(2n, 2m+1)$ is a solution of Pell's equation $x^2 - 3y^2 = 1$. As shown already, we obtain $2n + (2m+1)\sqrt{3} = (2+\sqrt{3})^l$. In order for n to be integral, l must be odd. It follows that $4n = (2+\sqrt{3})^{2k+1} + (2-\sqrt{3})^{2k+1}$. Finally,

   $$2n - 1 = \frac{(1+\sqrt{3})^2(2+\sqrt{3})^{2k} + (1-\sqrt{3})^2(2-\sqrt{3})^{2k} - 8}{4} = N^2,$$

   whereby N is an integer: $N = \frac{1}{2}\left((1+\sqrt{3})(2+\sqrt{3})^k + (1-\sqrt{3})(2-\sqrt{3})^k\right)$.

9. If n is an integer such that $3n + 1$ and $4n + 1$ are both squares, prove that n is a multiple of 56.

   Solution. Let us find all such n. Denoting $3n + 1 = a^2$ and $4n + 1 = b^2$ we have $(2a)^2 - 3b^2 = 1$.

   We shall find all solutions of $x^2 - 3b^2 = 1$ with an even $x = 2a$. The solutions of the Pell's equation $u^2 - 3v^2 = 1$ are given by $(u,v) = (u_k, v_k)$, where $u_k + v_k\sqrt{3} = (2+\sqrt{3})^k$. One easily sees that u_k is even if and only if k is odd. Thus $(x,b) = (u_{2k+1}, v_{2k+1})$, where we also have

   $$2u_{2k+1} = (2+\sqrt{3})^{2k+1} + (2-\sqrt{3})^{2k+1}.$$

It follows that $(a,b)=(\frac{1}{2}u_{2k+1},v_{2k+1})$ and $n=\frac{1}{3}(a^2-1)=\frac{1}{12}(u_{2k+1}^2-4)$, which yields

$$\begin{aligned}48n &= (7+4\sqrt{3})^{2k+1}+(7-4\sqrt{3})^{2k+1}-14\\ &= 2\left(7^{2k+1}-7+48\binom{2k+1}{2}7^{2k-1}+48^2\binom{2k+1}{2}7^{2k-3}+\cdots\right).\end{aligned}$$

We thus obtain a simpler expression for n, making the divisibility by 56 obvious:

$$n=\frac{7^{2k+1}-7}{24}+2\binom{2k+1}{2}7^{2k-1}+2\cdot 48\binom{2k+1}{2}7^{2k-3}+\cdots$$

10. Prove that the equation $x^2-dy^2=-1$ is solvable in integers if and only if so is $x^2-dy^2=-4$.

11. Let p be a prime. Prove that the equation $x^2-py^2=-1$ has integral solutions if and only if $p=2$ or $p\equiv 1 \pmod 4$.

    Solution. If the considered equation has a solution (x,y), then $p\mid x^2+1$; hence either $p=2$ or $p\equiv 1 \pmod 4$.

    For $p=2$, $x=y=1$ is a solution. We shall show that there is a solution for each prime $p=4t+1$. A natural starting point (and the only one we see!) is the existence of an integral solution (x_0,y_0) with $x_0,y_0\in\mathbb{N}$ to the corresponding Pell's equation: $x_0^2-py_0^2=1$. We observe that x_0 is odd: otherwise $y_0^2\equiv py_0^2\equiv 3 \pmod 4$. Thus in the relation $x_0^2-1=(x_0-1)(x_0+1)=py_0^2$, factors x_0+1 and x_0-1 have the greatest common divisor 2, and consequently one of them is a doubled square (to be denoted by $2x^2$) and the other one $2p$ times a square (to be denoted by $2py^2$). The case $x_0+1=2x^2$, $x_0-1=2py^2$ is impossible because it leads to a smaller solution of Pell's equation: $x^2-py^2=1$. It follows that $x_0-1=2x^2$, $x_0+1=2py^2$ and therefore $x^2-py^2=-1$.

12. If p is a prime of the form $4k+3$, show that exactly one of the equations $x^2-py^2=\pm 2$ has an integral solution.

    Solution. This is very similar to the previous problem. At most one has a solution. Now if (x_0,y_0) is the smallest solution of the corresponding Pell's equation, if $x_0\pm 1$ are not coprime, the equality $(x_0-1)(x_0+1)=py_0^2$ gives us $x_0\pm 1=2x^2$ and $x_0\mp 1=2py^2$, i.e. $x^2-py^2=\pm 1$, which is impossible in either case. Therefore $x_0\pm 1$ are coprime, which implies $x_0\pm 1=x^2$, $x_0\mp 1=py^2$ and $x^2-py^2=\pm 2$.

13. Prove that 3^n-2 is a square only for $n=1$ and $n=3$.

14. Prove that if $\dfrac{x^2+1}{y^2}+4$ is a perfect square, then this square equals 9.