Lecture Notes for International Mathematical Olympiad

PELL EQUATIONS

DAI WENHAN

1. An Introduction to Pell Equations

Definition 1.1 (Pell Equation)**.** The equation of the form $x^2 - Dy^2 = 1$ with $D \in \mathbb{Z}\backslash\{0\}$ is called *Pell equation*.

The solutions of Pell equation strongly depends on the choice of D.

- When $D < 0$, all solutions for $x^2 - Dy^2 = 1$ must be trivial, i.e., $(x, y) = (\pm 1, 0)$.
- When $D > 0$ is a perfect square, all solutions for $x^2 - Dy^2 = 1$ must be trivial as well.

Therefore, without loss of generality, we only study about the case where $D > 0$ and is not a perfect square. It can be proved that in these nontrivial case, the Pell equation always obtain at least one non-trivial integer solution (see, for example, [AG76]).

Definition 1.2 (Fundamental Solution)**.** Among all solutions for $x^2 - Dy^2 = 1$, the *fundamental solution* or the *minimal solution* is a non-trivial pair (x_0, y_0) such that $x_0 + \sqrt{D}y_0$ is minimal.

Proposition 1.3. *Suppose (x_0, y_0) is the fundamental solution for $x^2 - Dy^2 = 1$. Then for any integer solution (x, y), we have $x \geqslant x_0$ and $y \geqslant y_0$.*

Proof. Assume $x_0 > x$ for some x. Then

$$x_0^2 = Dy_0^2 + 1 > x^2 = Dy^2 + 1$$

which implies $y_0 > y$ at once. This contradicts to the assumption that $x_0 + \sqrt{D}y_0$ is the minimal. □

It's an essential step to find out the fundamental solution while solving the Pell equations. There are two ways to do this:

(1) taking trials for $y = 1, 2, \ldots$ until $1 + Dy^2$ is a perfect square;
(2) using the continued fraction (c.f. [Sho67, p. 204]).

Theorem 1.4. *The Pell equation $x^2 - Dy^2$ has infinitely many solutions of positive integers when $D > 0$ and D is a perfect square. All solutions of positive integers (x_n, y_n) with $n \in \mathbb{N}$ can be represented by the fundamental solution (x_0, y_0), say*

$$x_n + \sqrt{D}y_n = (x_0 + \sqrt{D}y_0)^n. \tag{$*$}$$

Proof. According to the binomial theorem, for $\sqrt{D} \in \mathbb{R}\backslash\mathbb{Q}$ and any $n \in \mathbb{N}$, if (x_n, y_n) satisfies $(*)$, we have

$$x_n - \sqrt{D}y_n = (x_0 - \sqrt{D}y_0)^n.$$

Multiplying with $(*)$,

$$x_n^2 - Dy_n^2 = (x_0 + \sqrt{D}y_0)^n (x_0 - \sqrt{D}y_0)^n = (x_0^2 - Dy_0^2)^2 = 1,$$

Date: August 1, 2022.

and hence (x_n, y_n) is a solution to $x^2 - Dy^2 = 1$. Suppose there exists some (x, y) that cannot be represented by (x_k, y_k), i.e., $x + \sqrt{D}y \neq (x_0 + \sqrt{D}y_0)^n$ for any n. As $x_0 + \sqrt{D}y_0 > 1$, there is a unique $r \in \mathbb{N}^*$ such that

$$(x_0 + \sqrt{D}y_0)^r < x + \sqrt{D}y < (x_0 + \sqrt{D}y_0)^{r+1}.$$

This is equivalent to

$$1 < \frac{x + \sqrt{D}y}{(x_0 + \sqrt{D}y_0)^r} = (x + \sqrt{D}y)(x_0 - \sqrt{D}y_0)^r < x_0 + \sqrt{D}y_0.$$

Here $1/(x_0 + \sqrt{D}y_0)^r = (x_0 - \sqrt{D}y_0)^r / (x_0^2 + \sqrt{D}y_0^2)^r = (x_0 - \sqrt{D}y_0)^r$. On the other hand, note that there are $X, Y \in \mathbb{Z}$ such that

$$(x + \sqrt{D}y)(x_0 - \sqrt{D}y_0)^r = X + \sqrt{D}Y.$$

Thus,

$$\begin{aligned} X - DY^2 &= (X + \sqrt{D}Y)(X - \sqrt{D}Y) \\ &= (x + \sqrt{D}y)(x_0 - \sqrt{D}y_0)^r (x - \sqrt{D}y)(x_0 + \sqrt{D}y_0)^r \\ &= (x^2 - Dy^2)(x_0^2 - Dy_0^2) = 1. \end{aligned}$$

Therefore, (X, Y) is a solution for the Pell equation, and then

$$1 < X + \sqrt{D}Y < x_0 + \sqrt{D}y_0 \quad \Rightarrow \quad 0 < X - \sqrt{D}Y = \frac{1}{X + \sqrt{D}Y} < 1$$

It boils down to verify that $X, Y \in \mathbb{N}^*$. Consider

- $(X + \sqrt{D}Y) + (X - \sqrt{D}Y) = 2X > 1 + 0 = 1$, hence $X > 0$ and then $X \in \mathbb{N}^*$;
- $\sqrt{D}Y > X - 1 \geqslant 0$, thus $Y \in \mathbb{N}^*$ again.

Therefore, $X - \sqrt{D}Y < 1 < X + \sqrt{D}Y < x_0 + \sqrt{D}y_0$ contradicts to the assumption that (x_0, y_0) is the minimal solution. □

Example 1.5. Here comes an example to understand Theorem 1.4. Given (x_0, y_0), we have

$$\begin{aligned} (x_0 \pm \sqrt{D}y_0)^3 &= x_0^3 \pm 3x_0^2 y_0 \sqrt{D} + 3x_0 D y_0^2 \pm D y_0^3 \sqrt{D} \\ &= (\underbrace{x_0^3 + 3x_0 D y_0^2}_{x_3}) - \sqrt{D}(\underbrace{3x_0^2 y_0 + D y_0}_{y_3}). \end{aligned}$$

Remarks 1.6. Here comes some properties on series $\{x_n\}$ and $\{y_n\}$.

(1) From two equations in Theorem 1.4 $(*)$, we get

$$\begin{aligned} x_n &= \frac{1}{2}((x_0 + \sqrt{D}y_0)^n + (x_0 - \sqrt{D}y_0)^n), \\ y_n &= \frac{1}{2\sqrt{D}}((x_0 + \sqrt{D}y_0)^n - (x_0 - \sqrt{D}y_0)^n). \end{aligned}$$

(2) By induction, for $n \geqslant 2$, we obtain recursive formulas read as

$$\begin{aligned} x_n &= 2x_0 x_{n-1} - x_{n-2}, \\ y_n &= 2x_0 y_{n-1} - y_{n-2}. \end{aligned}$$

These equations are hard to deduce but relatively easy to verify.

Definition 1.7 (Pell Equation, Type II)**.** The equation of the form $x^2 - Dy^2 = -1$ with $D \in \mathbb{Z} \backslash \{0\}$ is called *Pell equation of type II.*

The Pell equations of type II are more difficult to understand. We list out the following result without a proof.

Theorem 1.8. *Let $D \in \mathbb{N}^*$ be a non-perfect square integer. Suppose the equation $x^2 - Dy^2 = -1$ has a solution of positive integers. Then it has infinitely many solutions of positive integers, and all of them can be represented by the fundamental solution as*

$$x_n + \sqrt{D}y_n = (x_0 + \sqrt{D}y_0)^{2n+1}$$

for all $n \in \mathbb{N}$.

Remarks 1.9. We list out some remarks to understand Theorem 1.8.

(1) The equation $x^2 - Dy^2 = -1$ of type II does not necessarily have a solution even for those nice $D \in \mathbb{Z}$. However, the equation $x^2 - Dy^2 = 1$ of type I always has a solution under the same circumstance.
(2) The definition for a fundamental solution (x_0, y_0) of $x^2 - Dy^2 = -1$ is the same as before, i.e., the non-trivial solution such that $x + \sqrt{D}y$ is the minimal.
(3) It's a tricky and verbose problem on algebraic number theory to find out for which D the Pell equation of type II has a solution.

2. Problems and Examples

Problem 2.1. For $n \in \mathbb{N}$, it is called a triangular number if there exists some $k \in \mathbb{N}$ such that $n = 1 + 2 + \cdots + k$. Find out a triangular number N of 4 digits such that it is a perfect square as well.

Solution. Suppose $N = m^2 = k(k+1)/2$. This is equivalent to

$$(2k+1)^2 - 2(2m)^2 = x^2 - 2y^2 = 1, \quad x = 2k+1,\ y = 2m.$$

Note that the fundamental solution for $x^2 - 2y^2 = 1$ is $(x_0, y_0) = (3, 2)$. On the other hand, as m^2 has 4 digits, we see $32 \leqslant m \leqslant 99$ and then $64 \leqslant y \leqslant 198$. By Theorem 1.4,

$$x_2 + \sqrt{D}y_2 = (3 + 2\sqrt{2})^2 = 17 + 2\sqrt{2} \quad \Rightarrow \quad x_2 = 17,\ y_2 = 12.$$

Again, by Remarks 1.6 (2), we have the recursive formula $y_n = 2x_0y_{n-1} - y_{n-2} = 6y_{n-1} - y_{n-2}$. Given $(x_1, y_1) = (x_0, y_0) = (3, 2)$, we compute

$$y_3 = 70 > 64, \quad y_4 = 408 > 198.$$

Therefore, the only solution in need is $m = 70/2 = 35$ with $N = m^2 = 1225$. □

Problem 2.2. Find out the minimal positive integer $n > 1$ such that the arithmetic average of $1^2, 2^2, \ldots, n^2$ is a perfect square.

Solution. The condition is read as

$$\frac{1^2 + 2^2 + \cdots + n^2}{n} = \frac{(n+1)(2n+1)}{6} = m^2,$$

which is equivalent to $16n^2 + 24n + 8 = 3(4m)^2$. Thus,

$$(4n+3)^2 - 3(4m)^2 = x^2 - 3y^2 = 1, \quad x = 4n+3,\ y = 4m.$$

Its fundamental solution is given by $(x_0, y_0) = (x_1, y_1) = (2, 1)$. Hence

$$x_k = 4x_{k-1} - x_{k-2}, \quad x_1 = 2;$$
$$y_k = 4y_{k-1} - y_{k-2}, \quad y_1 = 1.$$

From this, we see a necessary condition $x_k \equiv -x_{k-2} \bmod 4$ and $y_k \equiv -y_{k-2} \bmod 4$. On the other hand, it is readily true that $x \equiv 3 \bmod 4$ and $y \equiv 0 \bmod 4$. The solution on k is $k \equiv 2 \bmod 4$.

- If $k = 2$, then $x_2 = 7 = 4n + 3$ with $n = 1$, which contradicts to $n > 1$.

- If $k=6$, we compute
$$\begin{aligned}x_6 &= 4x_5 - x_4 = 4(4x_4 - x_3) - x_4 = 15x_4 - 4x_3\\ &= 15(4x_3 - x_2) - 4x_3 = 56x_3 - 15x_2 = 56(4x_2 - x_1) - 15x_2\\ &= 209x_2 - 56x_1 = 1351,\end{aligned}$$
which implies that $4n+3=1351$ and then $n=337>1$.

Therefore, the anwser is $n=337$. □

Problem 2.3 (IMO 2001 Shortlist)**.** Consider the equation set
$$\begin{cases} x+y=z+u,\\ 2xy=zu.\end{cases}$$
Seek for the maximum of the real constant m such that for any solution (x,y,z,u) of positive integers for the equation set, $x\geqslant y$ always implies $m\leqslant x/y$.

Solution. We are to find out the lower bound of x/y. Firstly,
$$(x+y)^2 - 4\cdot 2xy = (z+u)^2 - 4\cdot zu \quad\Rightarrow\quad x^2 - 6xy + y^2 = (z-u)^2.$$
We can rewrite this formula in a homogeneous way, say
$$(\frac{x}{y})^2 - 6(\frac{x}{y}) + 1 = (\frac{z-u}{y})^2 \geqslant 0 \quad\Rightarrow\quad \frac{x}{y}\geqslant 3+2\sqrt{2}.$$
(Comment: note that $3+2\sqrt{2}\notin\mathbb{Q}$ but $x/y\in\mathbb{Q}$; therefore, consider to prove validity of the lower bound.) Suppose p is a prime divisor for $(z,u) := \gcd(z,u)$. Then $p\mid x$ and $p\mid y$ simultaneously. Without loss of generality, keeping the equation set invariant, we may suppose $(z,u)=1$. Here comes
$$(x+y)^2 - 2\cdot 2xy = (z+u)^2 - 2\cdot zu \quad\Rightarrow\quad (x-y)^2 = z^2+u^2.$$
As $(z,u)=1$, it is clear that $(z,u,x-y)$ is a primary pythagorean triple. This means the existence of a parametrization (again, may assume $2\mid u$):
$$u=2ab,\ z=a^2-b^2,\ x-y=a^2+b^2,\quad (a,b)=1.$$
Also, $x+y=z+u=a^2+2ab-b^2$, and hence $x=a^2+ab=a(a+b)$, $y=ab-b^2=b(a-b)$. Moreover,
$$z-u=a^2-b^2-2ab=(a-b)^2-2b^2.$$
The most important step is to set $z-u=1$ to make $(z-u)/y$ to be minimal. In case $z-u=1$ is satisfied, the solution $a-b=3$ with $b=2$ admit a Pell equation, say
$$(a-b)^2-2b^2=1.$$
According to Theorem 1.4, it has infinitely many solutions of positive integers so that $a-b$ and b can be sufficiently large as required. Consequently, y can be sufficiently large just so $y\to\infty$ is possible. It renders that
$$\frac{z-u}{y}\to 0 \quad\Rightarrow\quad \frac{x}{y}\to 3+2\sqrt{2}.$$
Hence we have proved that $m=3+2\sqrt{2}$ is the infimum for x/y. □

References

[AG76] William W Adams and Larry Joel Goldstein. *Introduction to number theory.* Prentice Hall, 1976.
[Sho67] James E Shockley. *Introduction to number theory.* Holt, Rinehart and Winston, 1967.

School of Mathematical Sciences, Peking University, 100871, Beijing, China
Email address: daiwenhan@pku.edu.cn