International Journal of Mathematical Sciences
Vol. 17, Nos. 3-4, July-December 2018, pp. 267-276

STUDY ON FUNDAMENTAL SOLUTION OF PELL'S EQUATION

Rajesh Kumar, Research Scholar, Deptt. of Mathematics, V.K.S. University, Ara (Bihar)

Abstract: We establish Study on Fundamental Solution of Pell's Equation $x^2 - dy^2 = \pm n$ where n is an integer. We obtained the complete solution of this equation, when $d \neq 0$.

Keywords: Diophantine Equation and Fundamental Solution.

3.1 INTRODUCTION

Now we consider some specific Diophantine equation and their integer solutions. Let $d \neq 0$ be a positive non square integer and n be a fixed positive integer. Then the Diophantine equation

$$x^2 - dy^2 = \pm n \tag{3.1}$$

is known as Pell's equation and is named after John Pell. Let us consider the equation

$$nx^2 + 1 = y^2 \tag{3.2}$$

and this equation arises naturally while we approximate $\sqrt{n}$ by rational numbers. Now we can also write this equation as $y^2 - nx^2 = 1$, where n is an integer and we are looking for integer solution, say (x, y).

This equation is called as Pell's equation.

The first mathematician to study this equation were Indian mathematicians Brahmagupta and Bhaskara.

Let us first note that

$$(b^2 - na^2)(d^2 - nc^2) = (bd + nac)^2 - n(bc + ad)^2 \tag{3.3}$$

and

$$(b^2 - na^2)(d^2 - nc^2) = (bd - nac)^2 - n(bc - ad)^2 \tag{3.4}$$

from this two equations we see that if $b^2 - na^2 = 1$ and $d^2 - nc^2 = 1$

$$(bd + nac)^2 - n(bc + ad)^2 = 1$$

$$(bd - nac)^2 - n(bc - ad)^2 = 1$$

so if (a, b) and (c, d) are solutions to Pell's equation then $(bc + ad, bd + nac)$ and $(bc - ad, bd - nac)$ are also solutions. This is important fact generalizes easily to give Brahmagupta's lemma.

3.2 BRAHMAGUPTA'S METHOD:

If (a, b) and (c, d) are integer solutions to Pell's equation of the form $na^2 + k = b^2$ and $nc^2 + k' = d^2$ respectively then $(bc + ad, bd + nac)$ and $(bc - ad, bd - nac)$ are both integer solution to the Pell's type equation

$$nx^2 + kk' = y^2 \tag{3.5}$$

Brahmagupta's lemma was discovered by himself in 628 AD.

The Proof that we given earlier is due to European Mathematician Euller in the Time of 17^{th} century.

We shall call this method as 'method of composition', in fact this method of composition allow Brahmagupta to make a number of fundamental discoveries regarding Pell's equation.

He deduced one property which is that if (a, b) satisfies Pell's method of composition to (a, b) and (a, b) then again we can applied the method of composition to (a, b) and $(2ab, b^2 + na^2)$. Brahmagupta immediately saw that form one equation of Pell's equation he could generate many solution. He also noted that using the similar argument we have just given, if $x = a$, $y = b$ is a solution of $nx^2 + k = y^2$ then applying method of composition to (a, b) and (a, b) gave $(2ab, b^2 + na^2)$. as a solution of $nx^2 + k = y^2$ and so dividing through by k we get

$$x = \frac{2ab}{k},\ y = \frac{b^2 + na^2}{k}$$

as a solution of Pell's equation $nx^2 + 1 = y^2$.

This values x, y do not look like integer if $k = 2$, then since (a, b) is a solution of $nx^2 + k = y^2$ we have $na^2 = b^2 - 2$. Thus $x = \dfrac{2ab}{2} = ab$, $y = \dfrac{2b^2 - 2}{2} = b^2 - 1$ which is an integer solution of Pell's equation.

If $k = -2$ then essentially the same argument works and while $k = 4, -4$ then a more complicated method, still it is based on method composition, shows that integer solution to Pell's equation can be found.

So Brahmagupta was able to show that if he can find (a, b) which nearly satisfies Pell's equation in the sense that $na^2 + k = b^2$ where $k = \pm 1, \pm 2, \pm 4$, Then he can find many integer solution to Pell's equation.

Example 3.2.1

Brahmagupta himself gives a solutions of Pell's equation

$$83x^2 + 1 = y^2 \tag{3.6}$$

Solution 3.2.2.

Here $a = 1$, $b = 9$ satisfies the equation $83.1^2 - 2 = 9^2$

So applying above method $x = \frac{2ab}{k}$, $y = \frac{b^2 + na^2}{k}$ is a solution to (3.6),

i.e, $x = \frac{2 \times 9}{2}$, $y = \frac{81 + 83 \times 1}{2}$ *i.e,* $x = 9$, $y = 82$ *i.e,* (9, 82) is a solution.

Then applying method of composition (9, 82), (9, 82) $(2ab, b^2 + na^2)$ is a solution *i.e,* $(2 \times 9 \times 82, 82 \times 82 + 83 \times 81) = (1476, 13447)$

Again applying method of composition to (9, 82), (1476, 13447) we get $x = ad + bc$, $y = bd + nac$ *i.e,* $x = 9 \times 13447 + 82 \times 1476 = 242055$, $y = 82 \times 13447 + 83 \times 9 \times 1476 = 2205226$

Again applying method of composition to (1476, 13447) and (242055, 2205226) $x = 6509827161$, $y = 5907347692$

Now applying (242055, 2205226) $x = 1067557198860$, $y = 972604342215$

Again applying method of composition to (242055, 2205226) and (39695544, 361643617)

$x = 175075291425879$, $y = 15950118138848202$

Therefore we have generate equation of solution (x, y)

3.3 CYCLIC METHOD

The next step was forwarded by mathematician Bhaskara in 1150. He discovered the cyclic method, called Chakravala method by Indian. This is a algorithm to produce a solution to a Pell's equation

$$nx^2 + 1 = y^2$$

Starting from a close pair (a, b) with $na^2 + k = b^2$

Here we assume that (a, b) are coprime, otherwise we can divide each by their gcd and get a closer solution with smaller k.

After that a and k are also coprime.

This method relies on a simple observation. Now let for any m, $(1, m)$ satisfy Pell's type equation $n.\ 1^2 + (m^2 - n) = m^2$.

Bhaskara applied the method of composition to the pair (a, b) and $(1, m)$ to get $am + b$, $bm + na$.

Now dividing by k

$$x = \frac{am + b}{k}, y = \frac{bm + na}{k}$$

is a solution to

$$nx^2 + \frac{m^2 - n}{k} = y^2$$

Since a, k are Prime to each other, we can choose m such that $am + b$ is divisible by k.

He knows that when m is choose so that $am + b$ is divisible by k then $m^2 - n$ and $bm + na$ are also divisible by k with such choice of therefore has the integer solution

$$x = \frac{am + b}{k},\ y = \frac{bm + na}{k}$$

To the Pell's type equation

$$nx^2 + \frac{m^2 - n}{k} = y^2$$

Where $\frac{m^2 - n}{k}$ is also an integer.

Next he knows there are infinitely m such that $am + b$ is divisible by k. so he choose the one which makes $(m^2 - n)$ as small as possible in absolute value. Then if $\frac{(m^2 - n)}{k}$ is one of $k = \pm1, \pm2, \pm4$, then we can apply Brahmagupta's method to find the solution to Pell's equation

$$nx^2 + 1 = y^2$$

If $\frac{(m^2 - n)}{k}$ is not one of these values then we have to repeat the process starting with the solution

$$x = \frac{am + b}{k},\ y = \frac{bm + na}{k}$$

to Pell type equation $nx^2 + \frac{m^2 - n}{k} = y^2$ in exactly the same way as we applied the process to $na^2 + k = b^2$.

However he knows that the process will end after a finite no. of steps and this happens when an equation of the form

$$nx^2 + t = y^2$$

is reach 0 where $t = \pm 1, \pm 2, \pm 4$.

Bhaskara gives an example in Bijaganita.

Example 3.3.1

$$6x^2 + 1 = y^2 \tag{3.7}$$

Solution 3.3.2.

We choose $a = 1$, $b = 8$ which satisfies the equation

$$61 \times 1^2 + 3 = 8^2$$

Now we choose the m so that k divides $(am + b)$. Here for that m, $\frac{m+8}{3}$ is an integer. Again we choose this m so that $m^2 - n$ that is $m^2 - 61$ is as small as possible.

Then taking $m = 7$ we get

$$x = \frac{am+b}{k} = \frac{7+8}{3} = 5$$

$$y = \frac{bm+na}{k} = \frac{8\times 7 + 61\times 1}{3} = 39$$

as a solution of Pell's equation $nx^2 + \frac{m^2-n}{k} = y^2$ *i.e,* $61x^2 + \frac{49-61}{3} = y^2$ that implies $61x^2 - 4 = y^2$.

Now we can apply Brahmagupta method to solve the equation and by Brahmagupta method solution is

$$x = 226153980,\ y = 1766319049$$

as the smallest to $6x^2 + 1 = y^2$

The next contribution to Pell's equation was made by mathematician Narayana in 14th century.

3.4 CONTINUED FRACTION METHOD

The equation

$$x^2 - dy^2 = \pm 1 \tag{3.8}$$

Where d > 0 is squarefree, arises naturally in trying to approximatite $\sqrt{d}$ by rational numbers. The techniques of this section are based on the continued fraction expansion of $\sqrt{d}$ and the norm identity in the integers $Z\left[\sqrt{d}\right]$

The continued fraction expansion of $\sqrt{d}$ is given by the following algorithm: see ([4])

1. The continued fraction has the form $[a_0, \overline{a_1, a_2 \ldots a_2, a_1, 2a_0}]$
2. The expansion of $\sqrt{d}$ is computed by

$$A_0 = 0 \quad B_0 = 1 \quad ak = \left[\frac{A_k + \sqrt{d}}{B_k}\right]$$

$$A_{k+1} = a_k B_k - A_k \quad B_{k+1} = \frac{d - A_{K+1}^2}{B_k}$$

3. The convergent $\frac{pk}{qk}$ of $\sqrt{d}$ satisfy

$$p_k^2 - dq_k^2 = (-1)^{(K+1)} \mathrm{B}_{k+1}$$

4. The shortest period Length m of $\sqrt{d}$ is the smallest positive m such that $B_m = 1$.

   Let $\mathrm{Z}\left[\sqrt{d}\right]$ be the numbers of the form $a + b\sqrt{d}$ for integers a and b. Then addition and multiplication are defined by

$$\left(a+b\sqrt{d}\right)+\left(x+y\sqrt{d}\right)=\left(a+x\right)+\left(b+y\right)\sqrt{d}$$

$$\left(a+b\sqrt{d}\right)\left(x+y\sqrt{d}\right)=\left(ax+dby\right)+\left(ay+bx\right)\sqrt{d}$$

   also the conjugate of $\propto = a + b\sqrt{d}$ is $\overline{\propto} = a - b\sqrt{d}$ and the norm is $N(a + b\sqrt{d}) = (a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - db^2$. Now we are in a way to solve the equation $x^2 - dy^2 = 1$ by considering x and y positive.

Theorem 3.4.1.

If p and q are positive integers satisfying the equation $p^2 - dq^2 = 1$, then $\frac{p}{q}$ is a convergent of $\sqrt{d}$.

Proof. If $p^2 - dq^2 = 1$, then, $(p + d\sqrt{d})(p - d\sqrt{d}) = 1$ and so

$$\left|p - q\sqrt{d}\right| = \left|\frac{1}{p + q\sqrt{d}}\right|$$

Dividing by q, we get $$\left|\frac{p}{q} - \sqrt{d}\right| = \frac{1}{q\left|p + d\sqrt{d}\right|}$$

Now, $p > q\sqrt{d}$ since $p^2 > dq^2$ and hence $p + q\sqrt{d} > 2q\sqrt{d}$.

Therefore

$$\left|\frac{p}{q} - \sqrt{d}\right| = \frac{1}{q\left|p + d\sqrt{d}\right|} < \frac{1}{q2q\sqrt{d}} = \frac{1}{2q^2\sqrt{d}}$$

Since $d > 1$, we get that $|\frac{p}{q} - \sqrt{d}| < \frac{1}{2q^2}$. Hence $\frac{p}{q}$ is a convergent of $\sqrt{d}$.

Theorem 3.4.2.

Let $\frac{p_k}{q_k}$ be the k th convergent of $\sqrt{d}$. If the period length m of $\sqrt{d}$ is even, then the solutions of $x^2 - dy^2 = 1$ are $x = p_{jm-1}$ and $y = q_{jm-1}$ for any j≥0. If the period length m of $\sqrt{d}$ is odd, then the solutions are $x = p_{jm-1}$ and $y = q_{jm-1}$ for j even. In particular, if d is not a perfect square, then the equation has infinitely many solutions. See ([4])

Proof. Using theorem (3.4.1), we see that every solution is a convergent. We know that $\frac{p_k}{q_k}$ satisfies $p_k^2 - dq_k^2 = (-1)^{K+1} B_{K+1}$.

if m is the period of the continued fraction, then $B_k = 1$ if and only if $m|k$.

Then we have $k = jm$ and substituting is equation we have

$$p_{jm-1}^2 - dq_{jm-1}^2 = (-1)^{jm} B_{jm} = (-1)^{jm}$$

If m is even, $(-1)^{jm} = 1$ and all the convergent $\frac{p_{jm-1}}{q_{jm-1}}$ give solution to equation. If m is odd, $(-1)^{jm} = 1$ when j is even.

Here we are giving an example to find solution by continued fraction method.

Example 3.4.3.

$$19x^2 + 1 = y^2 \tag{3.9}$$

Solution 3.4.4.

At first we have to first find out the continue fraction expansion of $\sqrt{19}$.

$$\frac{A_0 + \sqrt{19}}{B_0},\ A_0 = 0, B_0 = 1$$

$$A_{K+1} = a_k B_k - A_{k,} \quad B_{K+1} = \frac{\left(n - \left(A_{K+1}\right)2\right)}{Bk}$$

$$x_k = \frac{A_k + \sqrt{n}}{B_k}, \quad a_k = \left[x_k\right]$$

k	A_k	B_k	x_k	a_k
0	0	1	$\sqrt{19}$	4
1	4	3	$\frac{4+\sqrt{19}}{3}$	2
2	2	5	$\frac{2+\sqrt{19}}{5}$	1
3	3	2	$\frac{3+\sqrt{19}}{2}$	3
4	3	5	$\frac{3+\sqrt{19}}{5}$	1
5	2	3	$\frac{2+\sqrt{19}}{3}$	2
6	4	1	$\frac{4+\sqrt{19}}{1}$	8
7	4	3	$\frac{4+\sqrt{19}}{3}$	2
8	2	5	$\frac{2+\sqrt{19}}{5}$	1
9	3	2	$\frac{3+\sqrt{19}}{2}$	3

From the table we see that when $k = 8$, we obtain the same terms as when $k = 2$. Since the computation of A_k and B_k depends only on the previous terms, so the terms must repeat. Therefore the continued fraction is

$$\sqrt{19} = [4,2,1,3,1,2,8,2,1,3,\ldots] = [4,\overline{2,1,3,1,2,8}]$$

Since the period length is even, so the solutions are $x = p_{jm-1}$ and $y = q_{jm-1}$ for any $j \geq 0$.

k	0	1	2	3	4	5
$\frac{p_k}{q_k}$	$\frac{4}{1}$	$\frac{9}{2}$	$\frac{13}{3}$	$\frac{48}{11}$	$\frac{61}{14}$	$\frac{170}{39}$

since $\frac{p_s}{q_s} = \frac{170}{39}$, so

$$19.39^2 + 1 = 170^2$$

is the smallest nontrivial solution to find the infinite series of solution. Now let us take the power of $(170 + 39\sqrt{19})$

$$((170 + 39\sqrt{19})^2 = 57799 + 13260\sqrt{19})$$

$$x = 13260, y = 57799$$

Again taking the power, $(170 + 39\sqrt{19})^3 = 1965140 + 4508361\sqrt{19}$

So we get $x = 4508361$, $y = 196514$

Example 3.4.5

To verify the theorem (3.4.2), we give the following example.

$$x^2 - 13y^2 = 1 \tag{3.10}$$

Solution 3.4.6.

The continued fraction expansion of $\sqrt{13}$ is

$$\sqrt{13} = \left[3, \overline{1,1,1,1,6}\right] \tag{3.11}$$

and the period length is odd, so the solutions are $x = p_{5j-1}$ and $y = q_{5j-1}$ for j even. Also for j odd (p_{5j-1}, q_{5j-1}) givens solutions to $x^2 - 13y^2 = -1$. Now the convergents are

k	$\frac{p_k}{q_k}$	$p_k^2 - 13q_k^2$
0	$\frac{3}{1}$	–4
1	$\frac{4}{1}$	3
2	$\frac{7}{2}$	–3
3	$\frac{11}{3}$	4
4	$\frac{18}{5}$	–1
5	$\frac{119}{33}$	4

Contd...

6	$\frac{137}{38}$	–3
7	$\frac{256}{71}$	3
8	$\frac{393}{109}$	–4
9	$\frac{649}{180}$	1
10	$\frac{4287}{1189}$	–4
11	$\frac{4936}{1369}$	3
12	$\frac{9223}{2558}$	–3
13	$\frac{14159}{3927}$	4
14	$\frac{23382}{6485}$	–1

The Pell equation in (3.8) has infinitely many integer solutions (x_n, y_n) for $n \geq 1$ and first nontrivial positive integer solution (x_1, y_1) of this equation is called fundamental solution because all other solution can be easily derived from it. In fact if (x_1, y_1) is the fundamental solution of the equation $x^2 - dy^2 = 1$, then the nth positive solution of it that is (x_n, y_n) is defined by the equality

$$x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n \tag{3.12}$$

for integer $n \geq 2$. The methods for finding the fundamental solution have already discussed.

3.5 REFERENCES

[1] David M. Burton, "Elementary Number Theory", Tata McGraw-Hill, Sixth Edition (2011)

[2] Gareth A. Jones and J. Mary Jones, "Elementary Number Theory", Springer-Verlag London Limited (2007).

[3] Martin Erickson and Anthony Vazzana, "Introduction to Number Theory", Chapman and Hall/CRC (2010).

[4] Neville Robbins, "Beginning Number Theory", Narosa (2006).