# PELL'S EQUATION

A Project Report

Submitted by

PANKAJ KUMAR SHARMA

In partial fulfillment of the requirements

For award of the degree

Of

MASTER OF SCIENCE

IN

MATHEMATICS

UNDER GUIDANCE OF

Prof. G.K.PANDA

DEPARTMENT OF MATHEMATICS


NATIONAL INSTITUTE OF TECHNOLOGY

ROURKELA, ODISHA

# CERTIFICATE

This is to certify that the project report submitted by Mr. Pankaj Kumar Sharma to the National Institute of Technology, Rourkela, Odisha for the partial fulfillment of the requirements of M.Sc. degree in Mathematics is a bonafide review work carried out by him under my supervision and guidance. The content of this report in full or parts has not been submitted to any other Institute or University for the award of any degree or diploma.

Prof.G.K.PANDA

DEPARTMENT OF MATHEMATICS

NIT ROURKELA

# DECLARATION

I declare that the topic "PELL'S EQUATION" for my M.Sc Project has not been submitted by anyone in any other institution or university for award of any degree.

Place: PANKAJ KUMAR SHARMA

Date: Roll No: 410MA2109

# ACKNOWLEDGEMENT

I would like to express my deep appreciation to my guide Dr. G.K.PANDA, Professor and Head, Department of Mathematics, NIT Rourkela for the time, guidance, encouragement he has given me during this project period.

I would like to thank the faculty members of Department of Mathematics and Ph.D. scholar Mr. Sudhansu Sekhar Rout who helped me a lot for this project.

Thanks to all my friends and classmates who encourage me a lot in this project.

I owe my gratitude to my parents and brother, who supported for their blessings and inspiration.

PANKAJ KUMAR SHARMA

# CONTENTS

# INTRODUCTION

Number theory is that branch of mathematics that is concerned with the properties of numbers. For this reason, number theory, which has a 4000 years of rich history, has traditionally been considered as pure mathematics. The theory of numbers has always occupied a unique position in the world of mathematics. This is due to unquestionable historical importance of the subject. It is one of the few disciplines having demonstrable results that predate the very idea of a university or an academy. The natural numbers have been known to us for so long that mathematician Leopold Kronecker once remarked, "God created the natural numbers, and all the rest is the work of man". Far from being a gift from Heaven, number theory has a long and sometimes painful evolution.

The theory of continued fractions begins with Rafael Bombelli, the last of great algebraists of Renaissance Italy. In his L'Algebra Opera (1572) , Bombelli attempted to find square roots by using infinite continued fractions. One of the main uses of continued fraction is to find the approximate values of irrational numbers.

Srinivas Ramanujan has no rival in the history of mathematics. His contribution to number theory is quite significant. G.H.Hardy, commenting on Ramanujan's work, said "On this side (of Mathematics) most recently I have never met his equal, and I can only compare him with Euler or Jacobi".

Pell's equation $x^2 - dy^2 = 1$,was probably first studied in the case $x^2 - 2y^2 = 1$.Early mathematicians, upon discovering that $\sqrt{2}$ is irrational, realized that although one cannot solve the equation $x^2 - 2y^2 = 0$ in integers,one can at least solve the "next best things". The early investigators of Pell equation were the Indian mathematicians

Brahmagupta and Bhaskara. In particular Bhaskara studied Pell's equation for the values $d = 8,11,32,61$ and $67$ Bhaskara found the solution $x = 1776319049, y = 2261590,$ for $d = 61.$

Fermat was also interested in the Pell's equation and worked out some of the basic theories regarding Pell's equation. It was Lagrange who discovered the complete theory of the equation, $x^2 - dy^2 = 1$.Euler mistakenly named the equation to John Pell. He did so apparently because Pell was instrumental in writing a book containing these equations. Brahmagupta has left us with this intriguing challenge: "A person who can, within a year, solve $x^2 - 92y^2 = 1$ is a mathematician." In general Pell's equation is a Diophantine equation of the form $x^2 - dy^2 = 1$, where $d$ is a positive non square integer and has a long fascinating history and its applications are wide and Pell's equation always has the trivial solution $(x, y) = (1,0)$, and has infinite solutions and many problems can be solved using Pell's equation.

# Chapter-1

## PRELIMINARIES:

**Divisibility:** If $a$ and $b$ are two integers, then we say that $a$ divides $b$ and we write $a \mid b$ if $b = ka$ for some integer $k$.

**Division Algorithm:** Given two integers $a$ and $b$ with $b > 0$, there exists unique integers $q$ and $r$ satisfying

$$a = qb + r, \qquad 0 \leq r < b$$

The integers $q$ and $r$ are called quotient and remainder respectively in the division of $a$ by $b$.

Greatest Common Divisor: The greatest common divisor $(m, n)$ of integers $m$ and $n$ is the largest integer which divides both $m$ and $n$.

- Given integers $a$ and $b$, not both of which are zero, then there exist integers $x$ and $y$ such that

$$d = (a, b) = ax + by$$

- Euclid lemma: If $(a, b) = 1$ and $a \mid bc$, then $a \mid c$
- $m$ and $n$ are relatively prime if $(m, n) = 1$

**Euclidean Algorithm:** The Euclidean algorithm used to find the gcd of two integers, is the repeated application of division algorithm, starting with the number $a$ and $b$, and terminating when a remainder of $0$ occurs.

In general the Euclidean algorithm runs as follows:

$$a = bq_1 + r_1 \qquad 0 \leq r_1 < b,$$

$$b = r_1 q_2 + r_2 \qquad 0 \leq r_2 < r_1,$$

$r_1 = r_2q_2 + r_3$ $\quad 0 \leq r_3 < r_2,$

.

.

$r_i = r_{i+1}q_{i+2} + r_{i+2}$ $\quad 0 \leq r_{i+2} < r_{i+1},$

.

.

$r_{n-2} = r_{n-1}q_n + r_n$ $\quad 0 \leq r_n < r_{n-1},$

$r_{n-1} = r_nq_{n+1} + 0.$

Hence $r_n = (a, b)$.

Example: To calculate $d = (1492, 1066)$, we have

$$1492 = 1.1066 + 426$$

$$1066 = 2.426 + 214$$

$$426 = 1.214 + 212$$

$$214 = 1.212 + 2$$

$$212 = 106.2 + 0$$

The last non zero remainder is 2. So $d = 2$

**Linear Diophantine Equation:** A linear equation which is to be solved for integers is called a Diophantine equation.

The linear Diophantine equation of the form $ax + by = c$ has solution iff $(a, b) \mid c$.

Theorem1.1: *Let $a, b, c \in Z$. Consider the linear Diophantine equation $ax + by = c$.*

*a) If $(a, b) \nmid c$, there are no solutions.*

*b) If* $(a, b) \mid c$*, there are infinitely many solutions of the form*

$$x = \frac{b}{d}k + x_0 \ , y = -\frac{a}{d}k + y_{0,}$$

*Where* $(x_0, y_0)$ *is a particular solution and* $k \in \mathbb{Z}$*.*

Example: $6x + 9y = 21$.

Since $(6, 9) = 3$ and $3 \mid 21$, there are infinitely many solutions. By trial and error we find that, $x = -7, y = 7$ is a particular solution. Hence the general solution is given by

$x = 3k - 7, y = -2k + 7, k \in \mathbb{Z}$

Prime number: An integer $p > 1$ is called a prime number if its only positive divisors are 1 and $p$.

An integer greater than 1 that is not a prime is termed as composite.

**Fundamental Theorem of Arithmetic***: Every positive integer* $n > 1$ *can be expressed as a product of prime; this representation is unique, apart from the order in which the factors occur, i.e.* $n = p_1 p_2 \dots p_n$

Theorem 1.2: *There exists infinitely many primes.*

**Proof**: Suppose that $p_1, p_2, \dots, p_n$were the only primes. Let M be the product of these primes. Since $M + 1 > 1$, then there exists a prime $q$, such that $q \mid (M + 1)$. Since $(M + 1, M) = 1$, we know $q \nmid M$. Therefore $q \neq p_i$, for all $i$ such that $1 \leq i \leq n$ contrary to hypothesis. So there exist infinitely many primes. □

# Chapter-2

## CONTINUED FRACTION:

A continued fraction is an expression of the form

$$a_0 + \cfrac{b_1}{a_1 + \cfrac{b_2}{a_2 + \cfrac{b_3}{a_{3+\ldots}}}}$$

where $a_i$ and $b_i$ are either rational numbers, real numbers or complex numbers. If $b_i = 1$ for all $i$, then the expression is called a simple continued fraction. If the expression contains finitely many terms then it is called a finite continued fraction; otherwise it is called an infinite continued fraction. The number $a_i$ are called the partial quotients.

If the expression is truncated after $k$ partial quotients, then the value of the resulting expression is called the $k^{th}$ convergent of the continued fraction, and it is denoted by $C_k$. If $a_i$ and $b_i$ repeat cyclically, then the expression is called a periodic continued fraction. We express it as $[a_0, a_1, a_2, a_3, ....]$, if $a_0$ is an integer.

Example: $\frac{47}{17}$

By Euclidean algorithm

$$47 = 2.17 + 13$$

$$17 = 1.13 + 4$$

$$13 = 3.4 + 1$$

$$4 = 4.1 + 0$$

So, $\frac{47}{17} = 2 + \frac{1}{1+\frac{1}{3+\frac{1}{4}}} = 2 + \frac{1}{1+\frac{1}{3+\frac{1}{3+\frac{1}{1}}}}$

$$=[\,2;1,3,4] = [2;1,3,3,1].$$

So we noticed that the continued fraction expansion of a rational number is not unique.

$Note$: The $k^{th}$ convergent of the continued fraction $[a_0; a_1, a_2, a_{3,\ldots,} a_n]$ is $C_k = [a_0; a_1, a_2, a_{3,\ldots,} a_k]$ and for $k \geq n, C_k = [a_0; a_1, a_2, a_{3,\ldots,} a_n]$.

Theorem 2.1: *Let $a_0, a_1, \ldots, a_n$ be positive real numbers. Let*

$p_0 = a_0,$ $\qquad q_0 = 1$

$p_1 = a_1 a_0 + 1,$ $\qquad q_1 = a_1$

$p_k = a_k p_{k-1} + p_{k-2},$ $\qquad q_k = a_k q_{k-1} + q_{k-2}, \quad k \geq 2.$

*Then the $k^{th}$ convergent is given by* $C_k = \frac{p_k}{q_k}$.

**Proof:** We will prove this by induction on $k$. Since $c_0 = a_0$ and $c_1 = a_0 + \frac{1}{a_1} = \frac{(a_0 a_1 + 1)}{a_1}$. So, result holds for $k = 0$ and $k = 1$. Assume that the result is true for $k = m \geq 1$, then

$$[a_0; a_1, .., a_{m-1}, a_m, a_{m+1}] = [a_0; a_1, .., a_{m-1}, a_m + \frac{1}{a_{m+1}}]$$

Since the first $m$ partial quotients $(i.e\ a_0, a_1, a_{m-1})$ are same in both continued fraction, so we see that

$$\left[a_0; a_1, .., a_{m-1}, a_m + \frac{1}{a_{m+1}}\right] = \frac{\left(a_m + \frac{1}{a_{m+1}}\right) p_{m-1} + p_{m-2}}{\left(a_m + \frac{1}{a_{m+1}}\right) q_{m-1} + q_{m-2}}$$

$$c_{m+1} = \frac{a_m p_{m-1} + p_{m-2} + \frac{p_{m-1}}{a_{m+1}}}{a_m q_{m-1} + q_{m-2} + \frac{q_{m-1}}{a_{m+1}}}$$

$$= \frac{a_{m+1} p_m + p_{m-1}}{a_{m+1} q_m + q_{m-1}} = \frac{p_{m+1}}{q_{m+1}}$$

Hence the assertion for $k = m + 1$. □

Example: $\frac{19}{51}$ = [0; 2,1,2,6]

$p_0 = 0, q_0 = 1,\ p_1 = 0.2 + 1 = 1, q_1 = 2, p_2 = 1.1 + 0 = 1$
$q_2 = 1.2 + 1 = 3,\ p_3 = 2.1 + 1 = 3, q_3 = 2.3 + 2 = 8$

$p_4 = 6.3 + 1 = 19, q_4 = 6.8 + 3 = 51$ , so

$c_o = \frac{p_o}{q_o} = 0,\ \ c_1 = \frac{p_1}{q_1} = \frac{1}{2},\quad c_2 = \frac{p_2}{q_2} = \frac{1}{3},\quad c_3 = \frac{p_3}{q_3} = \frac{3}{8},$
$c_4 = \frac{p_4}{q_4} = \frac{19}{51}$ .

Theorem 2.2: *If* $C_k = \frac{p_k}{q_k}$ *is the* $k^{th}$ *convergent of the finite simple continued fraction* $[a_1, a_2, \dots, a_n]$ *then*

$$p_k q_{k-1} - q_k p_{k-1} = (-1)^{k-1},\ 1 \le k \le n.$$

**Proof:** We will prove this by induction. For $k = 1$,

$$p_1 q_0 - q_1 p_0 = (a_1 a_0 + 1) \cdot 1 - a_1 \cdot a_0 = 1 = (-1)^{1-1}$$

So result holds for $k = 1$. Now assume that it is true for $k = m$, where $1 \le m < n$. Then

$$p_{m+1} q_m - q_{m+1} p_m = (a_{m+1} p_m + p_{m-1}) q_m - (a_{m+1} q + q_{m-1}) p_m$$

$$= -(p_m q_{m-1} - q_m p_{m-1})$$

$$= -(-1)^{m-1}$$

$$= (-1)^{m}$$

showing that the formula holds for $n = m + 1$, Hence proved. □

Corollary 2.2.1: *For* $1 \leq k \leq n$, $p_k$ *and* $q_k$ *are relatively prime.*

**Proof:** If $d = \gcd(p_k, q_k)$, then $d \mid (-1)^{k-1}$. Since $d > 0, d = 1$.

Hence proved. □

Now we will see how to solve the linear Diophantine equation $ax + by = c$ using continued fraction.

Since, no solution of this equation exists if $d \nmid c$, where $d = (a, b)$, so there is no harm in assuming that $d \mid c$. For if $(a, b) = d > 1$, then $\frac{a}{d}x + \frac{b}{d}y = \frac{c}{d}$. Both equations have the same solution and in the latter case, we know that $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$. Notice that a solution of the equation $ax + by = c$, with $(a, b) = d$ may be obtained by solving first the Diophantine equation $ax + by = 1$ with $(a, b) = 1$.

If integer $x_0$ and $y_0$ can be found for which $ax_0 + by_0 = 1$, then multiplying both sides by $c$ we get,

$$a(cx_0) + b(cy_0) = c$$

Hence $x = cx_0$ and $y = cy_0$ is the of solution of $ax + by = c$. To find a pair of integer's $x$ and $y$ satisfying the equation

$ax + by = 1$, we have to find the simple continued fraction expansion of the rational number $\frac{a}{b}$ where, $\frac{a}{b} = [a_0, a_1, a_2, \ldots, a_n]$

The last two convergents of this continued fraction are

$$c_{n-1} = \frac{p_{n-1}}{q_{n-1}}$$

and,

$$c_n = \frac{p_n}{q_n} = \frac{a}{b}.$$

As $(p_n, q_n) = 1 = (a, b)$, we have $p_n = a$ and $q_n = b$. Then

$$p_n q_{n-1} - q_n p_{n-1} = (-1)^{n-1}$$

which implies,

$$aq_{n-1} - bp_{n-1} = (-1)^{n-1}.$$

Thus, with $x = q_{n-1}$ and $y = -p_{n-1}$, so

$$ax + by = (-1)^{n-1}.$$

If $n$ is odd, then $ax + by = 1$, has particular solution

$$x_0 = q_{n-1}, y_0 = -p_{n-1}$$

If $n$ is even, then

$$x_0 = -q_{n-1}, y_0 = p_{n-1}$$

And the general solution is,

$$x = x_0 + bt, y = y_0 - at, t = 0, \pm 1, \pm 2, \ldots$$

Now let's solve the linear Diophantine equation

$$172x + 20y = 1000$$

by using simple continued fraction.

We have, $(172,20) = 4$.

$172x + 20y = 1000 \Rightarrow 43x + 5y = 250.$

Firstly we have to find a particular solution to $43x + 5y = 1.$

$\frac{43}{5} = [8; 1,1,2].$

The convergent are

$$c_0 = \frac{8}{1}, c_1 = \frac{9}{1}, c_2 = \frac{17}{2}, c_3 = \frac{43}{5}$$

$p_2 = 17, q_2 = 2, p_3 = 43, q_3 = 5$

Now, $p_3 q_2 - q_3 p_2 = (-1)^{3-1}$

implying that, $43.2 - 5.17 = 1$

multiplying both sides by 250, we get

$43.500 + 5.(-4250) = 250.$

So, the particular solution is given by $x_0 = 500, y_0 = -4250$ and

the general solution is given by

$x = 500 + 5t\ , y = -4250 - 43t\ , t = 0, \pm 1, \pm 2 \ldots$

## Periodic Continued Fraction:

$\sqrt{2} = [1; \overline{2}]$ $\sqrt{3} = [1; \overline{1,2}]$

Here we see that partial quotients 2 and 1, 2 repeat indefinitely, such fractions are called periodic. We write a periodic continued fraction as,

$[a_0; a_1, .., a_m, b_1, .. b_n, b_1, .., b_n, \ldots] = [a_0; a_1, .., a_m, \overline{b_1, \ldots, b_n}]$. Here, $b_1, b_2, \ldots, b_n$ is the period of the expansion and the length of the period is $n$.

Example: $[3; \overline{1,2,16}]$ , is a continued fraction whose period 1,2,1,6 has length 4.

*Note*: If $[a_0; a_1, a_2, \ldots.]$ is an infinite continued fraction with positive terms, then its value is an irrational number. Every irrational number $x$ has a unique infinite continued fraction expansion $[a_0; a_1, a_2, \ldots.]$ whose terms are given recursively by

$$x_0 = x \text{ and } a_k = [x_k]\,, \quad x_{k+1} = \frac{1}{x_k - a_k} \text{ for } k \geq 0$$

Example: $x = \sqrt{23} \approx 4 \cdot 8$

$$x_0 = \sqrt{23} = 4 + \left(\sqrt{23} - 4\right), \qquad a_0 = 4$$

$$x_1 = \frac{1}{x_0 - [x_0]} = 1 + \frac{\sqrt{23} - 3}{7}, \qquad a_1 = 1$$

$$x_2 = \frac{1}{x_1 - [x_1]} = 3 + \frac{\sqrt{23} - 4}{2}, \qquad a_2 = 3$$

$$x_3 = \frac{1}{x_2 - [x_2]} = 1 + \frac{\sqrt{23} - 3}{2}, \qquad a_3 = 1$$

$$x_4 = \frac{1}{x_3 - [x_3]} = 8 + \left(\sqrt{23} - 4\right), \qquad a_4 = 8$$

So, $\sqrt{23} = [4; \overline{1,3,1,8}]$.

# Chapter-3

**PELL'S EQUATION:** $x^2 - dy^2 = 1$.

John Pell (1611-1685) was an English mathematician who taught mathematics in Holland, at the universities of Amsterdam and Breda in 1640's. Pell's equation has a long fascinating history. Its first recorded appearance is in the cattle problem of Archimedes. This problem involves eight different kinds of cattle and ask the reader to determine how many there are of each kind. After facing a lot of problem's it finally reduced to solving the Pell's equation $x^2 - 4729494y^2 = 1$. The first significant progress in solving the Pell's equation was made in India as early as A.D. 628, by Brahmagupta. Brahmagupta described how to use the known solution to a Pell's equation to create new solutions and Bhaskaracharya in 1150 A.D. gave a method of solving Pell's equation. The modern European history of Pell's equation begins in 1657 when Fermat challenged his fellow mathematician to solve the equation $x^2 - 61y^2 = 1$ several of them found the smallest solution, which was $(x, y) = (1766319049, 226153980)$ and William Brouncker in 1657 described a general method for solving Pell's equation. Brouncker found the solution $(32188120829134849, 1819380158564160)$.

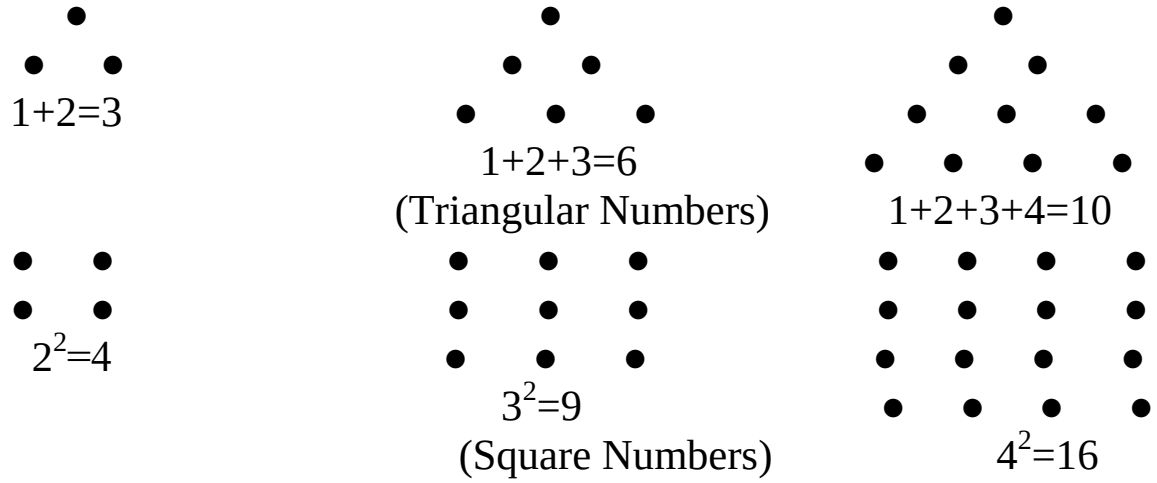
J. Wallis described Brounckers method in a book on algebra and number theory and Wallis and Fermat both asserted that the Pell's equation always has a solution. Euler mistakenly thought that the method in Wallis book was due to John Pell, and so Euler assigned the equation the name Pell's equation. But John Pell has nothing to do with the so called Pell's equation.

**Problems Leading To Pell's Equation:** One of the main reasons for the popularity of Pell's equation is the fact that many natural

questions that one might ask about integer's leads to a quadratic equation in two variables, which can be casted as a Pell's equation.

## Square Triangular Numbers:

The numbers which can be arranged in a shape of triangle is called triangular numbers, whereas the numbers which can be arranged in a shape of square are called square numbers.




The $m^{th}$ triangular number is = $\frac{m(m+1)}{2}$ and the $n^{th}$ square number = $n^2$

We observe that the sum of two adjacent triangular numbers is square.

But what about the case when an individual triangular number is square?

So, the square triangular numbers are solution to the equation

$n^2 = \frac{m(m+1)}{2}$ ; $m, n \in \mathbb{Z}^+$.

Multiplying both sides by 8 we get

$8n^2 = 4m^2 + 4m = (2m+1)^2 - 1.$

Letting, $x = 2m + 1, y = 2n$, we have

$2y^2 = x^2 - 1 \Rightarrow x^2 - 2y^2 = 1$

Solution to $x^2 - 2y^2 = 1$, gives square-triangular numbers with $m = \frac{x-1}{2}\ and\ n = \frac{y}{2}$. How to solve the Diophantine equation $x^2 - 2y^2 = 1$?

There are triangular numbers that differ from a square by 1 such as

$3 = 2^2 - 1, 10 = 3^2 + 1, 15 = 4^2 - 1, 120 = 11^2 - 1.$

Are there other such triangular numbers? This leads to solving the equation

$\frac{x(x+1)}{2} = y^2 - 1$ This implies, $(2x + 1)^2 = 8y^2 - 7.$

## BRAHMAGUPTA'S METHOD:

$nx^2 + 1 = y^2$ (Pell's equations) leading to $y^2 - nx^2 = 1.$

Identity: $(b^2 - na^2)(d^2 - nc^2) = (bd \pm nac)^2 - n(bc \pm ad)^2.$

From this we observe that if $(b^2 - na^2)$ and $(d^2 - nc^2)$ are both 1, then $(bd \pm nac)^2 - n(bc \pm ad)^2 = 1$, i.e. if $(a, b)\ and\ (c, d)$ are solution to pell equation then $(bc \pm ad, bd \pm nac)$ is also a solution.

Brahmagupta's Lemma:

*If $(a, b) and\ (c, d)$ are integer solution of pell type equation of the form $na^2 + k = b^2 and\ nc^2 + k' = d^2$, then $(bc \pm ad, bd \pm nac)$ are both integer solution of Pell type equation $nx^2 + kk' = y^2$, using the method of composition, if $(a, b)$ satisfies pells equation, then so does $(2ab, b^2 + na^2)$ which is obtained by composing $(a, b)$ with itself. Another solution can be obtained by composing $(a, b)$ with $(2ab, b^2 + na^2)$.*

## Solving Pell's Equation Using Brahmagupta's Method:

By Brahmagupta's lemma if $(a, b)$ is solution of $nx^2 + k = y^2$, then composing $(a, b)$ with itself gives us $(2ab, b^2 + na^2)$ as a solution of $nx^2 + k = y^2$ and dividing by $k$, we get

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

Which is a solution to the Pell's equation $nx^2 + 1 = y^2$.

For most values of $k$ this idea is not helpful because $x, y$ are not integers, but when $k \; is \; \pm 1, \pm 2$ or $\pm 4$ this idea helps a lot.

When $k = 2$, as $(a, b)$ is solution of $nx^2 + k = y^2$ then, $na^2 = b^2 - 2$,

so, $x = \frac{2ab}{2} = ab, y = \frac{b^2+na^2}{2} = \frac{b^2+b^2-2}{2} = \frac{2b^2-2}{2} = b^2 - 1.$

For $k = -2, na^2 = b^2 + 2$ and

$x = \frac{2ab}{-2} = -ab, \; y = \frac{b^2+b^2+2}{-2} = -b^2 - 1.$

For $k = 4, -4$ we can get solutions to the Pell's equation by method of composing, but it's too much complicated. So Brahmagupta was able to show that if we can find $(a, b)$ which nearly satisfies Pell's equation in the sense $na^2 + k = b^2$ where $k = \pm 1, \pm 2, \pm 4$,then we can find many integer solutions to Pell's equation.

EXAMPLE: Brahmagupta's solution of the Pell's equation

$83x^2 + 1 = y^2.$

Here $a = 1, b = 9$ satisfy the equation $83.1^2 - 2 = 9^2$. So applying the above method, we find that, $x = \frac{2ab}{k}$, $y = \frac{b^2+na^2}{k}$

is a solution to,

$83x^2 + 1 = y^2$.

i.e., $= \frac{2\times9}{2} = 9$ , $y = \frac{81+83\times1}{2} = 82.$

i.e., $(9, 82)$ is a solution. Applying method of composition to $(9, 82)$ and $(9, 82)$ we get,

$(2\times 9 \times 82, 82 \times 82 + 83 \times 81)$ = (1476, 13447).

Again applying method of composition to (9, 82) and (1476, 13447).

we have, $x = 9 \times 13447 + 82 \times 1476 = 242055.$

$$y = 82 \times 13447 + 83 \times 9 \times 1476 = 2205226.$$

By applying again and again the method of composition, we can generate further solutions $(x, y)$.

## Results on Pell's Equation:

The Pell equation is a Diophantine equation of the form $x^2 - dy^2 = 1$. Given $d$, we want to find all integer pairs $(x, y)$ that satisfy the equation. Since any solution $(x, y)$ yields multiple solution $(\pm x, \pm y)$, we restrict ourselves to those solutions where $x$ and $y$ are positive integers. We generally take $d$ to be a positive non-square integer; otherwise there are only uninteresting solutions. If $d < 0$, then $(x, y)$ = $(\pm1,0)$, in the case $d < -1$ and $(x, y) = (0, \pm1)$ or $(\pm1,0)$ in the case $d = -1$, if $d = 0$, then $x = \pm1$ ($y$ arbitrary) and if $d$ is non – zero square ,then $dy^2$ and $x^2$ are consecutive squares, implying that $(x, y)$ = $(\pm1,0)$.

Notice that the Pell equation always has the trivial solution

$(x, y) = (1,0)$.

The following result is well known: *If* $\frac{p_n}{q_n}$ *is the* $n^{th}$ *convergent to the irrational number* $x$*, then*

$$| x - \frac{P_n}{P_n} | < \frac{1}{q_{n+1}q_n} \leq \frac{1}{{q_n}^2}.$$

Theorem 3.1: *If* $\frac{p}{q}$ *is a convergent of the continued fraction expansion of* $\sqrt{d}$ *then,* $x = p, y = q$ *is a solution of one of the equation* $x^2 - dy^2 = k$ *where* $|k| < 1+2\sqrt{d}$.

**Proof:** If $\frac{p}{q}$ is a convergent of $\sqrt{d}$, then

$$|\sqrt{d} - \frac{p}{q}| < \frac{1}{q^2}$$

and, therefore

$$\left|p - q\sqrt{d}\right| < \frac{1}{q}.$$

Now

$$\left|p + q\sqrt{d}\right| = \left|\left(p - q\sqrt{d}\right) + 2q\sqrt{d}\right| \leq \left|p - q\sqrt{d}\right| + \left|2q\sqrt{d}\right|$$

$$< \frac{1}{q} + 2q\sqrt{d} \leq \left(1 + 2\sqrt{d}\right)q.$$

These two inequalities combine to yield

$$|p^2 - dq^2| = \left|p - q\sqrt{d}\right|\left|p + q\sqrt{d}\right| < \frac{1}{q}\left(1 + 2\sqrt{d}\right)q = 1 + 2\sqrt{d}. \quad \square$$

Example: Let $d = 7$.

$\sqrt{7} = [2, \overline{1,1,1,4}]$,The first two convergent of $\sqrt{7}$ are $\frac{2}{1}, \frac{3}{1}, \frac{5}{2}, \frac{8}{3}, \ldots$

Now calculating, $p_n^2 - 7q_n^2$, we find that

$$2^2 - 7 \cdot 1^2 = -3, 3^2 - 7 \cdot 1^2 = 2, 5^2 - 7 \cdot 2^2 = -3, 8^2 - 7 \cdot 3^2 = 1.$$

Hence $x = 8$, $y = 3$ provides a positive solution of $x^2 - 7y^2 = 1$.

Note: If $d$ is a positive integer that is not a perfect square, then the continued fraction expansion of $\sqrt{d}$ necessarily has the form $\sqrt{d} = [a_0, \overline{a_1, a_2, a_3, \dots, a_3, a_2, a_1, 2a_0}]$.

Example: $\sqrt{19} = [4, \overline{2,1,3,1,2,8}], \sqrt{73} = [8, \overline{1,1,5,5,1,1,16}]$.

If the length of the period of the continued fraction expansion of $\sqrt{d}$ is $n$, then the fundamental solution of the equation $x^2 - dy^2 = 1$ is given by $x = p_{n-1}, y = q_{n-1}$,when $n$ is even and by $x = p_{2n-1}, y = q_{2n-1}$, when $n$ is odd. Finding the fundamental solution may become a difficult task, as the value of the fundamental solution may be very large, even for comparatively small values of $d$. For example the equation

$x^2 - 991y^2 = 1$, has the fundamental solution

$x$=379516400906811930638014896080, and

$y$=12055735790331359447442538767.

The solution is even worse with $x^2 - 1000099y^2 = 1$, where the smallest positive integer has 1118 digits. So, everything depends upon the continued fraction expansion of $\sqrt{d}$ and in case of $\sqrt{1000099}$, the period has 2174 terms. There might be possibilities that the solution of $x^2 - dy^2 = 1$ may be small for a given value of $d$ and very large for succeeding values of $d$. For example the equation $x^2 - 61y^2 = 1$, whose fundamental solution is given by $x = 1766319049$, $y = 226153980$. But with the case $d = 60$, where the solution is $x = 31, y = 4$ and with $d = 62$, where the solution is $x = 63, y = 8$.

From any solution of $x^2 - dy^2 = 1$, we can obtain infinitely many solutions. Let $(x_1, y_1)$ be a solution of $x^2 - dy^2 = 1$. Then we can generate another solution by the following process:

$$x_1{}^2 - dy_1{}^2 = 1$$

$$\left(x_1 + y_1\sqrt{d}\right)\left(x_1 - y_1\sqrt{d}\right) = 1$$

$$(x_1 + y_1\sqrt{d})^2(x_1 - y_1\sqrt{d})^2 = 1$$

$$\left(x_1{}^2 + 2x_1y_1\sqrt{d} + dy_1{}^2\right)\left(x_1{}^2 - 2x_1y_1\sqrt{d} + dy_1{}^2\right) = 1$$

$$\left((x_1{}^2 + dy_1{}^2) + (2x_1y_1)\sqrt{d}\right)((x_1{}^2 + dy_1{}^2) - (2x_1y_1)\sqrt{d}) = 1$$

$$(x_1{}^2 + dy_1{}^2)^2 - d(2x_1y_1)^2 = 1.$$

We see that we have got a equation which is nothing but a Pell's Equation and $(x_1{}^2 + dy_1{}^2, 2x_1y_1)$ is a solution. Applying the process repeatedly we can get as many solution as we desire.

Alternatively, suppose we consider integer powers of $(x_1 + y_1\sqrt{d})$

$$\left(x_1 + y_1\sqrt{d}\right)^n = x_1{}^n + c_1\sqrt{d}x_1{}^{n-1} + c_2dx_1{}^{n-2}y_1{}^2 +$$

$$c_3d^{\frac{3}{2}}x_1{}^{n-3}y_1{}^3 + \ldots\ldots + d^{\frac{n}{2}}y_1{}^n$$

$$= (x_1{}^n + c_2dx_1{}^{n-2}y_1{}^2 + \ldots.) +$$

$$\sqrt{d}(c_1x_1{}^{n-1} + c_3x_1{}^{n-3}y_1{}^3 + \ldots.)$$

$$= x_n + y_n\sqrt{d}$$

where $c_i$ are the binomial coefficient, $c_i = \binom{n}{i}$.

Theorem 3.2: *Let* $(x_1, y_1)$ *be the fundamental solution of* $x^2 - dy^2 = 1$. *Then every pair of integers* $(x_n, y_n)$ *defined by the condition*

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

*is also a positive solution,* $n = 1,2,3, \ldots$ .

**Proof:** $x_n - y_n\sqrt{d} = (x_1 - y_1\sqrt{d})^n$

Further, because $x_1$ and $y_1$are positive $x_n$ and $y_n$ are both positive integers. Since $x_1, y_1$is a solution of $x^2 - dy^2 = 1$,we have

$$x_n^2 - dy_n^2 = \left(x_n + y_n\sqrt{d}\right)\left(x_n - y_n\sqrt{d}\right)$$

$$= \left(x_n + y_n\sqrt{d}\right)^n \left(x_n - y_n\sqrt{d}\right)^n$$

$$= (x_1^2 - dy_1^2)^n.$$

Hence, $(x_n, y_n)$ is a solution.

Example: $x^2 - 35y^2 = 1$

$x_1 = 6$, $y_1 = 1$, forms the fundamental solution. Now

$x_2 + y_2\sqrt{35} = \left(6 + \sqrt{35}\right)^2 = 71 + 12\sqrt{35}$.

So, $x_2 = 71, y_2 = 12$, which implies $(x_2, y_2)$ is a solution since,

$$71^2 - 35 \cdot 1^2 = 5041 - 5040 = 1.$$

$x_3 + y_3\sqrt{35} = (6 + \sqrt{35})^3 = 846 + 143\sqrt{35}$.

So, $x_3 = 846, y_3 = 143$.

$$846^2 - 35 \cdot 143^2 = 715716 - 715715 = 1.$$

In this way we can generate infinitely many solutions.

Note: If $(x_1, y_1)$ is the fundamental solution of $x^2 - dy^2 = 1$, then the solutions $(x_n, y_n)$ is also given by

$$x_n = \frac{1}{2}(x_1 + y_1\sqrt{d})^n + \frac{1}{2}(x_1 - y_1\sqrt{d})^n,$$

$$y_n = \frac{1}{2\sqrt{d}}(x_1 + y_1\sqrt{d})^n - \frac{1}{2\sqrt{d}}(x_1 - y_1\sqrt{d})^n.$$

Theorem 3.3: *If* $x_1 > 1, y_1 \geq 1$ *, and* $x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n$ *, then* $x_{n+1} > x_n$ *and* $y_{n+1} > y_n$ *for positive n.*

**Proof:** We will prove this by induction, observe that

$x_2 = {x_1}^2 + d{y_1}^2$ and $y_2 = 2x_1y_1$. Since $x_1 > 1, y_1 \geq 1$ and $d$ is a positive integer it is clear that $x_2 > x_1$ , $y_2 > y_1$. So, the result holds for $n = 1$.

Now assume the solution $(x_n, y_n)$ with $x_n$ *and* $y_n$ positive integers greater than 1. We have,

$$\begin{aligned} x_{n+1} + y_{n+1}\sqrt{d} &= (x_1 + y_1\sqrt{d})^{n+1} \\ &= (x_1 + y_1\sqrt{d})(x_1 + y_1\sqrt{d})^n \\ &= \left(x_1 + y_1\sqrt{d}\right)(x_n + y_n\sqrt{d}) \\ &= (x_1x_n + dy_1y_n) + (x_1y_n + x_ny_1)\sqrt{d} \end{aligned}$$

Therefore, $x_{n+1} = x_1x_n + dy_1y_n$ and $y_{n+1} = x_1y_n + x_ny_1$. We know that, $x_1x_n > x_n$ and $dy_1y_n > 0$, so $x_{n+1} = x_1x_n + dy_1y_n > x_n$, also $x_1y_n > y_n$ and $x_ny_1 > 0$, implies that

$$y_{n+1} = x_1y_n + x_ny_1 > y_n.$$

Therefore, we have $x_{n+1} > x_n$ and $y_{n+1} > y_n$. □

# Chapter-4

## ASSOCIATED PELL'S EQUATION:

The equation $x^2 - dy^2 = -1$ is called associated Pell's equation or, negative Pell's equation. Let $t$ be the length of the period the continued fraction expansion of $\sqrt{d}$. If $t$ is even, then $x^2 - dy^2 = -1$ has no solution.

If $t$ is odd, then $x^2 - dy^2 = -1$ has infinitely many solutions and all given by $(x_n, y_n) = (p_{(2n-1)t-1}, q_{(2n-1)t-1})$.

Example: The equation $x^2 - 7y^2 = -1$ has no solution, since $\sqrt{7} = [2; \overline{1,1,1,4}]$ so $t = 4$. Again $x^2 - 41y^2 = -1$ has solution, since $\sqrt{41} = [6; \overline{2,2,12}]$; so $t = 3$. The first two such solutions are

$(x_1, y_1) = (p_2, q_2) = (32,5)$.

$(x_2, y_2) = (p_8, q_8) = (131168, 20485)$.

## PELL NUMBERS:

The Pell number is defined by the recurrence relation

$$P_n = \begin{cases} 0, & if\ n = 0 \\ 1, & if\ n = 1 \\ 2P_{n-1} + P_{n-2}, & otherwise \end{cases}$$

That is, the Pell numbers sequence starts with 0 and 1, and then each Pell number is the sum of twice the previous Pell number and the Pell number before that. The first few terms of the sequence are $0,1,2,5,12,29,70,169,408,985,2378, \ldots\ldots$

The Pell number can also be expressed by the closed form

$$P_n = \frac{(1+\sqrt{2})^n - (1-\sqrt{2})^n}{2\sqrt{2}}$$

**PELL PRIME**: A Pell prime is a Pell number that is prime. The first few Pell primes are $2,5,29,5741$, ...

A Pell number $P_n$ can only be prime if $n$ itself is prime.

**PELL- LUCAS NUMBER**:

The Pell-Lucas numbers are defined by the recurrence relation

$$Q_n = \begin{cases} 2, & if\ n = 0 \\ 2, & if\ n = 1 \\ 2Q_{n-1} + Q_{n-2}, & otherwise \end{cases}$$

That is, the first two numbers in the sequence are both 2, and each successive number in formed by adding twice the previous Pell-Lucas number to the Pell-Lucas number before that, or, by adding the next Pell number to the previous Pell number. The first few terms of the sequence are $2, 2, 6, 14, 34, 82, 198, 478$, ...

The Pell-Lucas numbers can be expressed by the closed form $Q_n = (1+\sqrt{2})^n + (1-\sqrt{2})^n$.

The Pell-Lucas numbers are all even.

**HALF COMPANION PELL NUMBERS** ($H_n$):

$$H_n = \begin{cases} 1, & if\ n = 0 \\ H_{n-1} + 2P_{n-1}, & otherwise \end{cases}$$

$$P_n = \begin{cases} 0, & if\ n = 0 \\ H_{n-1} + P_{n-1}, & otherwise \end{cases}$$

# Chapter 5

## APPLICATIONS OF PELL'S EQUATION:

1) (Double equations): Find $t \in \mathbb{Z}$, such that $10t + 9 = x^2$ and $5t + 4 = y^2$

Solution: We have, $t = \frac{x^2-9}{10} = \frac{y^2-4}{5}$

implying that,

$$5\left\{\frac{x^2-9}{10}\right\} + 4 = y^2,$$

leads to,

$x^2 - 2y^2 = 1$, which is a Pell's equation with $d = 2$.

Solutions are listed in the following table:

| | | | | | | |
|---|---|---|---|---|---|---|
| $x$ | 3 | 17 | 99 | 577 | 3363 | 19601 |
| $y$ | 2 | 12 | 70 | 408 | 2378 | 13860 |
| $t$ | 0 | 28 | | 33292 | 1130976 | |

2) Rational approximation to square roots we cannot write $\sqrt{d} = \frac{x}{y}$, with $x, y \in \mathbb{Z}$,$\sqrt{d}$ is irrational. But

$x^2 - dy^2 = 1$

implies,

$$\left(\frac{x}{y}\right)^2 = d + \frac{1}{y^2} \approx d$$

so, Pell solutions lead to good rational approximation to $\sqrt{d}$.

Example: The fourth solution to $x^2 - 2y^2 = 1$ is $(x, y) = (577, 408)$ and $\frac{577}{408} = 1 \cdot 4142156$, while $\sqrt{2} = 1 \cdot 4142135$.

3) Sums of consecutive integers.

Example:

$$1 + 2 = 3, \quad 1 + 2 + \cdots + 14 = 15 + \cdots + 20$$

In general if we have,

$1 + 2 + \cdots + k = (k + 1) + \cdots + l$, then

$$\frac{(1+k)k}{2} = \frac{(k+1+l)(l-k)}{2}$$

leading to,

$$2k^2 + 2k = l^2 + l$$

and,

$$2\left(\left(k + \frac{1}{2}\right)^2 - \frac{1}{4}\right) = \left(l + \frac{1}{2}\right)^2 - \frac{1}{4},$$

which finally simplifies to,

$(2l + 1)^2 - 2(2k + 1)^2 = -1$, which is a associated Pell's equation and can be written as,

$$x^2 - 2y^2 = -1, \;\; x, y > 0, x = 2l + 1, y = 2k + 1$$

$x^2 - 2y^2 = -1$, with both $x$ and $y$ odd.

The solutions are listed below

| $x$ | 1 | 7 | 41 | 239 | 1393 | 8119 |
|---|---|---|---|---|---|---|
| $y$ | 1 | 5 | 29 | 169 | 985 | 5741 |

| | | | | | | |
|---|---|---|---|---|---|---|
| $k = \frac{y-1}{2}$ | 0 | 2 | 14 | 84 | 492 | 2870 |
| $l = \frac{x-1}{2}$ | 0 | 3 | 20 | 119 | 696 | 4059 |

So, $1 + 2 + \cdots + 84 = 85 + \cdots 119.$

4) Pythagorean triangle with consecutive legs, like $(3,4,5), (20,21,29),\ldots$

In general we are interested in solving $m^2 + (m+1)^2 = n^2$

Clearly, $n^2$ is odd, so $n$ is odd.

$$2m^2 + 2m + 1 = n^2$$

implies,

$$2(m^2 + m) + 1 = n^2 \Rightarrow 2\left(\left(m + \frac{1}{2}\right)^2 - \frac{1}{4}\right) + 1 = n^2$$

which gives,

$$(2m+1)^2 + 1 = 2n^2$$

and finally,

$$(2m+1)^2 - 2n^2 = -1$$

which is an associated Pell's equation.

So, $m^2 + (m+1)^2 = n^2 \Leftrightarrow (2m+1)^2 - 2n^2 = -1$

The solutions are listed in the following table.

| | | | | | | |
|---|---|---|---|---|---|---|
| $x$ | 1 | 7 | 41 | 239 | 1393 | 8119 |
| $y$ | 1 | 5 | 29 | 169 | 985 | 5741 |
| $m = \frac{x-1}{2}$ | 0 | 3 | 20 | 119 | 696 | 4059 |
| $n = y$ | 1 | 5 | 29 | 169 | 985 | 5741 |

$$3^2 + 4^2 = 5^2$$

$$20^2 + 21^2 = 29^2$$

$$119^2 + 120^+ = 169^2$$

5) Consecutive Heronian triangles

Example: The $3, 4, 5$ right triangle has area 6.

$$A = \sqrt{s(s-a)(s-b)(s-c)}, \qquad s = \frac{a+b+c}{2}$$

Find Heronian triangle with consecutive sides $a-1, a, a+1$, and thus, $s = \frac{3a}{2}$

$$A^2 = s(s-a)(s-a+1)(s-a-1)$$

$$A^2 = \frac{3a}{2} \cdot \frac{a}{2} \cdot \frac{a+2}{2} \cdot \frac{a-2}{2}$$

which implies,

$(4A)^2 = 3a^2(a^2-4)$. Then $a$ is even say $a = 2x$

so,

$A^2 = 3x^2(x^2-1)$.

Unique factorization $\Rightarrow x^2 - 1 = 3y^2$

$\Rightarrow x^2 - 3y^2 = 1, \quad a = 2x, \qquad A = 3xy$

| | | | | | | |
|---|---|---|---|---|---|---|
| $x$ | 2 | 7 | 26 | 97 | 362 | 1351 |
| $y$ | 1 | 4 | 15 | 56 | 209 | 780 |
| $a$ | 4 | 14 | 52 | 194 | 724 | 2702 |
| $A$ | 6 | 84 | 1170 | 16926 | 226974 | 3161340 |

So, we have triangles with sides $3, 4, 5$ ($area$ 6); $13, 14, 15$ ($area$ 84); $51, 52, 53$ ($area$ 1170) and so on.

# 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).