Diophantine Equation

A Project Report

submitted by

Sagar Panda

in partial fulfilment of the requirements

for the award of the degree

of

MASTER OF SCIENCE

IN MATHEMATICS

2011

DEPARTMENT OF MATHEMATICS

NATIONAL INSTITUTE OF TECHNOLOGY ROURKELA

ROURKELA, ORISSA-769008

CERTIFICATE

This is to certify that the Project Report entitled **"Diophantine Equation"** submitted by *Sagar Panda* to National Institute of Technology Rourkela, Orissa for the partial fulfilment of the requirements of M.Sc. degree in Mathematics is a bonafide record of review work carried out by him under my supervision and guidance. The content of this report, in full or in parts, has not been submitted to any other Institute or University for the award of any degree or diploma.

(G.K. Panda)
Professor
Department of Mathematics
NIT Rourkela

DECLARATION

I declare that the topic '*Diophantine equation*' for my M.Sc. degree has not been submitted in any other institution or university for the award of any other degree or diploma.

Place:	Sagar Panda
Date:	Roll No. 409MA2071

ACKNOWLEDGEMENT

I would like to warmly acknowledge and express my deep sense of gratitude and indebtedness to my guide **Prof. G.K. Panda**, Department of Mathematics, NIT Rourkela, Orissa, for his keen guidance, constant encouragement and prudent suggestions during the course of my study and preparation of the final manuscript of this Project.

I would like to thank the faculty members of Department of Mathematics for allowing me to work for this Project in the computer laboratory and for their cooperation. Also I am grateful to my senior Sudhansu Sekhar Rout, research scholar, for his timely help during my work.

My heartfelt thanks to all my friends for their invaluable co-operation and constant inspiration during my Project work.

I owe a special debt gratitude to my revered parents, my brother, sister for their blessings and inspirations.

Rourkela,769008

May, 2011 **Sagar Panda**

CONTENTS

INTRODUCTION AND SUMMARY

There is a quote by the famous mathematician Carl Friedrich Gauss $(1777-1855)$: "Mathematics is the queen of all sciences, and number theory is the queen of mathematics." Number theory, or higher arithmetic is the study of those properties of integers and rational numbers, which go beyond the ordinary manipulations of everyday arithmetic.

Throughout history, almost every major civilization has been fascinated by the properties of integers and has produced number theorists and ancient and medieval times, these were usually geometers, or more generally scholars, calendar calculators, astronomers, astrologers, priests or magicians. From the oldest number theoretical record we have a tablet from Babylonia,a table of right triangles with integer sides, that is, positive integer solutions to $x^2 + y^2 = z^2$. Some of these solutions are too large for us to believe that they discovered by trial and error in those days. The Babylonian scholars knew the Pythagorean Theorem well over a millennium before Pythagoras and were also able to compute with large numbers.

Euclid and Diophantus of Alexandria (about $300-200 B.C.$) are the best known number theorists of ancient times and Euclid's contribution consists of thirteen books, three of them are about number theory of the positive integers, but everything is stated in a geometric language. Among these important results, Euclid's contributions are the properties of divisibility of numbers including the idea of odd and even numbers, and an algorithm for finding the greatest common divisor of two numbers. He derived formulas for the sum of a finite geometric progression and for all Pythagorean triples he also introduced the notion of a prime number and showed that if a prime number divides a product of two numbers, it must divide at least one of them. He proved the infinitude of primes in the same way we are doing till today. One of the most famous mathematical problems of all time in

Diophantine analysis is Fermat's last theorem , which states that the Diophantine equation $x^n + y^n = z^n$ has no solution in positive integers x, y and z if $n > 3$. Pierre de Fermat $(1601 - 1665)$ was a judge in Toulouse, France and also a very serious amateur mathematician. One evening, reading a copy of Diophantus' Arithmetica, newly rediscovered and translated from Greek to Latin, he came on a theorem about Pythagorean triplets. In the margin of the book he wrote "It is impossible to separate a cube into two cubes, or a fourth power into two fourth powers, or, in general, any power higher than the second into two like powers. I have discovered a truly marvelous proof of this result, which, this margin is too narrow to contain." Fermat left no proof of the conjecture for all n, but he proved the special case $n = 4$. After that this reduced the problem to proving the theorem for all exponents n that are odd prime numbers. Over the next two centuries $(1637 - 1839)$, the conjecture was proved for only the first three odd primes $(3, 5,$ and $7)$, although Sophie Germain $(1776 - 1831)$ proved a special case for all primes less than 100 and in the mid-19th century, Ernst Kummer $(1810 - 1893)$ proved the theorem for a large (probably infinite) class of primes known as regular. On the base of Kummer's work and using sophisticated computer studies, other mathematicians were able to prove the conjecture for all primes up to four million. Despite much progress in special cases, the problem remained unsolved until British mathematician Andrew Wiles, working at Princeton University, announced his solution in 1992 and corrected in 1995 . Wiles' proof, not only settled an old mathematical problem, but it also opened the doors to new areas of research thought with the introduction of new ideas and techniques on Number theory.

In the first chapter we have given some definations, theorems, lemmas, on Elementary Number Theory. This brief discussion is useful for next discussion on the main topic.

We know that there are two type of Diophantine equation i.e., (i) Linear

Diophantine equation, (ii) Non-linear Diophantine equation. In the second chapter we have discussed about the solutions of both kind of Diophantine equation. Here we have given the necessary and sufficient condition for existence the solution of a Linear Diophantine equation and also discussed about the Non-linear Diophantine equation and discussed Fermat's Last theorem. Pell's equation is a special type of Diophantine equation. The history of Pell's equation is very interesting. In the last section we have given some methods to find the fundamental solution of the Pell's equation.

CHAPTER 1

Prelimnaries of Number Theory

In this chapter we recall some definitions and known results on elementary number theory. This chapter serves as base and background for the study of subsequent chapters. We shall keep on referring back to it as and when required.

Division Algorithm: Let a and b be two integers, where $b > 0$ then there exist unique q and r such that $a = bq + r, 0 \leq r < b$.

Definition 1.0.1. (Divisibility) An integer a is said to be divisible by an integer $d \neq 0$ if there exist some integer c such that $a = dc$.

Definition 1.0.2. If a and b are integers, not both zero, then the greatest common divisor of a and b, denoted by $gcd(a, b)$ is the positive integer d satisfying

1. $d \mid a$ and $d \mid b$
2. if $c \mid a$ and $c \mid b$ then $c \mid d$

Theorem 1.0.3. *Let a, b be two integers, not both zero, then there exist integers p, q such that $gcd(a, b) = ap + bq$.*

Euclidean Algorithm:see([5]) Euclidean algorithm is an method of finding the greatest common divisor of two given integers. This is the repeated application of the division algorithm

Let a and b two integers whose gcd is required. Since $gcd(a, b) = gcd(|a|, |b|)$, it is enough to assume that a, b are positive integers.

Without loss of generality, we assume $a > b > 0$. Now by division algorithm, $a = bq_1 + r_1$, where $0 \leq r_1 < b$.

If it happens that $r_1 = 0$, then $b \mid a$ and $gcd(a, b) = b$.

If $r_1 \neq 0$, by division algorithm $b = r_1q_2 + r_2$, where $0 \leq r_2 < r_1$.
If $r_2 = 0$, the process stops. If the $r_2 \neq 0$ by division algorithm $r_1 = r_2q_3+r_3$, where $0 \leq r_3 < r_2$.
The process continues until some zero remainder appears. This must happen because the remainders $r_1, r_2, r_3, ...$ form a decreasing sequence of integers and since $r_1 < b$, the sequence contains at most b non-negative integers. Let us assume that $r_{n+1} = 0$ and r_n is the last non-zero remainder.
We have the following relation

$$\begin{aligned}
&a = bq_1 + r_1, \quad 0 < r_1 < b\\
&b = r_1q_2 + r_2, \quad 0 < r_2 < r_1\\
&r_1 = r_2q_3 + r_3, \quad 0 < r_3 < r_2\\
&\cdots \quad \cdots \quad \cdots \quad \cdots\\
&r_{n-2} = r_{n-1}q_n + r_n, \quad 0 < r_n < r_{n-1}\\
&r_{n-1} = r_nq_{n+1} + 0
\end{aligned}$$

Therefore $gcd(a, b) = r_n$.
Fundamental theorem of Arithmetic: Any positive integer is either 1, or prime, or it can be expressed as a product of primes, the representation being unique except for the order of the prime factors.
Congruence: Let m be a fixed positive integer. Two integers a and b are said to be congruent modulo m if $a - b$ is divisible be m and symbolically this is denoted by $a \equiv b(\text{mod } m)$.
Some properties of Congruence:

1. $a \equiv a(\text{mod } m)$
2. If $a \equiv b(\text{mod } m)$, then $b \equiv a(\text{mod } m)$
3. If $a \equiv b(\text{mod } m)$, $b \equiv c \ (\text{mod } m)$ then $a \equiv c(\text{mod } m)$

4. If $a \equiv b(\text{mod } m)$, then for any integer c

   $(a+c) \equiv (b+c)(\text{mod } m); \quad ac \equiv bc(\text{mod } m)$

Polynomial Congruence: Let $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n \;\; (n \geq 1)$, be a polynomial with integer coefficients $a_0, a_1, \cdots, a_n$ with a_0 not congruent to 0 modulo m. Then $f(x) \equiv 0(\text{mod } m)$ is said to be a polynomial congruent modulo m of degree n.

Linear Congruence: A polynomial congruence of degree 1 is said to be a linear congruence.

The general form of a linear congruence modulo a positive integer $m \neq 0$ is $ax \equiv b(\text{mod } m)$, where ax is not congruent to 0 modulo m.

Chinese Remainder Theorem: See([5])Let $m_1, m_2, \cdots, m_r$ be positive integers such that $\gcd(m_i, m_j) = 1$ for $i \neq j$. Then the system of linear congruences

$$\begin{aligned} x &\equiv c_1(mod \;\; m_1) \\ x &\equiv c_2(mod \;\; m_2) \\ \vdots \;\; & \;\; \vdots \\ x &\equiv c_r(mod \;\; m_r) \end{aligned}$$

has a simultaneous solution which is unique modulo $m_1m_2 \cdots m_r$.

Continued fraction: See([4]) An expression $a_0 + \frac{b1}{a_1 + \frac{b_2}{a_2 + \frac{b_3}{\ddots \frac{b_{n-1}}{a_{n-1} + \frac{b_n}{a_n}}}}}$ is called a continued fraction.

Simple Continued fraction: See([4]) A continued fraction is called a simple continued fraction if all the b_i's are 1 and the a_i's are integers satisfying $a_1, a_2, \cdots \geq 1$. Simple continued fraction is denoted by $[a_0, a_1, \cdots, a_n]$, that is, $[a_0, a_1, \cdots, a_n] = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{\ddots \frac{1}{a_{n-1} + \frac{1}{a_n}}}}}$

In this notation , $\frac{181}{101} = [1, 1, 3, 1, 4, 4]$.

Remark 1.0.1. See([4])A real number α can be expressed as a simple continued fraction if and only if α is rational.

Convergent of simple continued fraction: See([4]) We determine the kth convergent C_k of the simple continued fraction $[a_0, a_1, \cdots, a_n]$ to be $C_k = [a_0, a_1, \cdots, a_k]$ for $k \leq n$.

Example 1.0.4.

The convergents of the simple continued fraction $\frac{181}{101} = [1, 1, 3, 1, 4, 4]$ are

$$\begin{aligned}
C_0 &= [1] = 1 \\
C_1 &= [1, 1] = 1 + \frac{1}{1} = 2 \\
C_2 &= [1, 1, 3] = 1 + \frac{1}{1 + \frac{1}{3}} = \frac{7}{4} \\
C_3 &= [1, 1, 3, 1] = \frac{9}{5} \\
C_4 &= [1, 1, 3, 1, 4] = \frac{43}{24} \\
C_5 &= [1, 1, 3, 1, 4, 4] = \frac{181}{101}
\end{aligned}$$

Remark 1.0.2. See([4]) For the kth convergent of the continued fraction $[a_0, a_1, \cdots, a_n]$, the numerator p_k and denominator q_k satisfies the recurrence relation

$$p_k = a_k p_{k-1} + p_{k-2} \tag{1.1}$$

$$q_k = a_k q_{k-1} + q_{k-2} \tag{1.2}$$

with initial values

$$p_0 = a_0, \quad p_1 = a_1 a_0 + 1, \quad q_0 = 1, \quad q_1 = a_1$$

Remark 1.0.3. See([4])Let $C_k = \frac{p_k}{q_k}$ be the kth convergent of $[a_0, a_1, \cdots, a_n]$. Then

$$p_k q_{k-1} - q_k p_{k-1} = (-1)^{k-1} \tag{1.3}$$

$$p_k q_{k-2} - q_k p_{k-2} = (-1)^k a_k \tag{1.4}$$

CHAPTER 2

Diophantine Equation

2.1 Linear Diophantine equation

An equation in one or more unknowns which is to be solved in integers is called Diophantine Equation, named after the Greek Mathematician Diophantus.See([2])
A Linear Diophantine equation of the form $ax + by = c$ may have many solutions in integers or may not have even a single solution.

2.2 Necessary and sufficient condition for existence of Linear Diophantine equation

If a, b, c are integers and a,b are not both zero, then the linear diophantine equation $ax + by = c$ has an integral solution if and only if $gcd(a, b)$ is a divisor of c.

Proof. Let one integral solution of the equation $ax+by = c$ be (x_1, y_1). Then $ax_1 + by_1 = c$, where (x_1, y_1) are integers. Let $gcd(a, b) = d$ and so $d \mid a$ and $d \mid b$ which implies $d \mid (ax_1 + by_1)$,i.e.,$d \mid c$.
conversly, let $gcd(a, b)$ be a divisor of c. Let $gcd(a, b) = d$ and so $a = dm$,$b = dn$ where m, n are integers prime to each other. Let $c = dp$ where p is an integer. Now since m, n are prime to each other, there exist integers u, v such that $mu + nv = 1$. Then

$$dmup + dnvp = dp$$
$$\Rightarrow a(up) + b(vp) = c$$

This implies that (up, vp) is a solution of the equation $ax + by = c$ where up and vp are integers . Hence the equation $ax + by = c$ has an integral solution. □

Theorem 2.2.1. *The linear Diophantine equation $ax+by=c$ has a solution if and only if $d \mid c$,where $d = gcd(a,b)$ and if (x_0, y_0) be any particular solution of the equation, then all other solutions will be*

$$x = x_0 + (\frac{b}{d})t \qquad y = y_0 - (\frac{a}{d})t$$

where t is an arbitrary integer.

Proof. To prove the second part of the theorem, let us suppose that (x_0, y_0) be a known solution of the given equation. Now if $x', y^{'}$ is any other solution, then

$$ax_0 + by_0 = c = ax^{'} + by^{'}$$

which is equivalent to

$$a(x^{'} - x_0) = b(y_0 - y^{'})$$

So there exist relatively prime integers r and s such that $a = dr, b = ds$. Substituting these value into the last equation and canceling the common factor d, we get $r(x^{'} - x_0) = s(y_0 - y^{'})$. Then $r \mid s(y_0 - y^{'})$, with $gcd(r,s) = 1$. Using Euclid's lemma, we get $r \mid (y_0 - y^{'})$; or in other words $(y_0 - y^{'}) = rt$ for some integer t and so $(x^{'} - x_0) = st$. From this we get $x^{'} = x_0 + st = x_0 + (\frac{b}{d})t$, $y^{'} = y_0 - rt = y_0 - (\frac{a}{d})t$ which satisfy the Diophantine equation

$$\begin{aligned} ax^{'} + by^{'} &= a[x_0 + (\frac{b}{d})t] + b[y_0 - (\frac{a}{d})t] \\ &= (ax_0 + by_0) + (\frac{ab}{d} - \frac{ab}{d})t \\ &= c + 0 \cdot t \\ &= c \end{aligned}$$

Hence there are infinite number of solutions of the given equation, one for each value of t. □

Example 2.2.2.

Let us take the linear Diophantine equation

$$172r + 20s = 1000$$

Solution 2.2.3. First applying the Euclidean's Algorithm we find that

$$\begin{aligned}
&172 = 8 \cdot 20 + 12\\
&20 = 1 \cdot 12 + 8\\
&12 = 1 \cdot 8 + 4\\
&8 = 2 \cdot 4.
\end{aligned}$$

Therefore $gcd(172, 20) = 4$. Now, since $4 \mid 1000$, a solution to this equation exists. To obtain the integer 4 as a linear combination of 172 and 20, we work backward through the previous calculations, as follows:

$$\begin{aligned}
4 &= 12 - 8\\
&= 12 - (20 - 12)\\
&= 2 \cdot 12 - 20\\
&= 2(172 - 8 \cdot 20) - 20\\
&= 2 \cdot 172 + (-17)20
\end{aligned}$$

Multiplying this relation by 250, we get

$$1000 = 250 \cdot 4 = 250[2 \cdot 172 + (-17)20] = 500 \cdot 172 + (-4250)20$$

So $r = 500$ and $s = -4250$ provide one solution to the Diophantine equation. All other solutions are

$$r = 500 + (\frac{20}{4})t = 500 + 5t \qquad s = -4250 - (\frac{172}{4})t = -4250 - 43t$$

for some integer t and for positive integers solutions, if exist , t must be chosen to satisfy simultaneously the inequalities

$$5t + 500 > 0, \qquad -43t - 4250 > 0$$

or, $\quad -98\frac{36}{43} > t > -100$

Next, we are looking for the non trivial solution of the nonlinear Diophantine equation.

2.3 Fermat's Last Theorem

The equation

$$x^n + y^n = z^n \tag{2.1}$$

where n is an integer greater than 2, has no integral solutions, except the trivial solutions in which one of the variables is 0.See([3])

The theorem had never been proved for all n. Later this has been resolved and proved for all n. In this chapter we are giving the solution of Fermat's last theorem i.e. the equation (2.1) is soluble for $n = 2$ and also the equation (2.1) has no integral solution for $n = 3$ and 4.

Theorem 2.3.1. *The general solution of the equation*

$$x^2 + y^2 = z^2 \tag{2.2}$$

satisfying the conditions

$$x > 0,\ y > 0,\ z > 0,\ (x, y) = 1,\ 2 \mid x, \tag{2.3}$$

is

$$x = 2ab,\ y = a^2 - b^2,\ z = a^2 + b^2, \tag{2.4}$$

where a, b are integers and

$$(a, b) = 1, a > b > 0, \tag{2.5}$$

There ia a one to one correspondence between different values of a, b and different values of x, y, z.

Proof. First, we assume that $x^2 + y^2 = z^2$ and $x > 0,\ y > 0,\ z > 0,\ (x, y) = 1,\ 2 \mid x$. Now since $2 \mid x$ and $(x, y) = 1$, y and z are odd and $(y, z) = 1$. So $\frac{1}{2}(z - y)$ and $\frac{1}{2}(z + y)$ are integral and

$$(\frac{z-y}{2}, \frac{z+y}{2}) = 1$$

Then by (2.2),

$$(\frac{x}{2})^2 = (\frac{z-y}{2}, \frac{z+y}{2}) = 1$$

and the two factors on the right, being coprime, must both be squares. So

$$\frac{z+y}{2} = a^2, \qquad \frac{z-y}{2} = b^2$$

where

$$a > 0, \quad b > 0, \quad a > b, \quad (a,b) = 1$$

Also

$$a + b \equiv (a^2 + b^2) = z \equiv 1(mod 2)$$

where a and b are of opposite parity. Therefore any solution of (2.2), satisfying (2.3), is of the form (2.4); and a and b are of opposite parity and satisfy (2.5).

Next, we assume that a and b are of opposite parity and satisfy (2.5). Then

$$x^2 + y^2 = 4a^2b^2 + (a^2 - b^2)^2 = (a^2 + b^2)^2 = z^2,$$

$$x > 0, \quad y > 0, \quad z > 0, \quad 2 \mid x$$

If $(x, y) = d$, then $d \mid z$, and so

$$d \mid y = (a^2 - b^2), d \mid z = (a^2 + b^2)$$

Therefore $d \mid 2a^2, d \mid 2b^2$. Since $(a, b) = 1$, d must be 1 or 2, and the second alternative is excluded because y is odd. Hence $(x, y) = 1$ and if y and z are given, a^2 and b^2 are uniquely determined, so that different values of x, y, and z correspond to different values of a and b. □

Theorem 2.3.2. *There are no positive integral solutions of the equation*

$$x^4 + y^4 = z^2 \tag{2.6}$$

Proof. Let u be the least number for which

$$x^4 + y^4 = u^2 \quad (x > 0, y > 0, u > 0) \tag{2.7}$$

has a solution. Then $(x, y) = 1$, otherwise we can divide through by $(x, y)^4$ and so replace u by a smaller number. Therefore at least one of x and y is odd, and $u^2 = x^4 + y^4 \equiv 1$ or $2(\text{mod}4)$.

Since $u^2 \equiv 2(\text{mod}4)$ is impossible, so u is odd, and one of x and y is even.

Now if x is even, then by (2.3.1),

$x^2 = 2ab, y^2 = a^2 - b^2, u = a^2 + b^2$,

$a > 0, \quad b > 0, \quad (a, b) = 1$ and a and b are of opposite parity. Again if a is even and b is odd, then

$y^2 \equiv (-1)(\text{mod}4)$ which is impossible; so a is odd and b is even, say $b = 2c$.

Next we get

$$(\frac{1}{2}x)^2 = ac \qquad (a, c) = 1$$

and so

$$a = d^2, c = f^2, d > 0, f > 0, \quad (d, f) = 1$$

and d is odd. Therefore

$$y^2 = a^2 - b^2 = d^4 - 4f^4$$

$$(2f^2)^2 + y^2 = (d^2)^2$$

and no two of $2f^2, y, d^2$ have a common factor.

Now by applying theorem (2.3.1) again, we obtain

$$2f^2 = 2lm, d^2 = l^2 + m^2, l > 0, m > 0, (l, m) = 1.$$

Since

$$f^2 = lm, \quad (l, m) = 1$$

we get

$$l = r^2, m = s^2 \quad (r > 0, s > 0)$$

and so

$$r^4 + s^4 = d^2.$$

But

$$d \leq d^2 = a \leq a^2 < a^2 + b^2 = u$$

and u is not the least number for which the equation (2.7) is possible. This is a contradiction which proves the theorem. □

2.4 Pythagorean triples and the unit circles

We have already described all the solutions to

$$x^2 + y^2 = z^2 \tag{2.8}$$

in whole numbers x, y and z. Now if we divide this equation by z^2, we obtain

$$(\frac{x}{z})^2 + (\frac{y}{z})^2 = 1 \tag{2.9}$$

and so the pair of rational numbers $(\frac{x}{z}, \frac{y}{z})$ is a solution to the equation

$$u^2 + v^2 = 1 \tag{2.10}$$

Therefore there are four rational solutions to the equation $u^2 + v^2 = 1$. see([4])These are $(\pm 1, 0)$ and $(0, \pm 1)$. Now if (x_0, y_0) is a point on the circle with rational coordinates, then the slope of the line joining (u_0, v_0) to $(-1, 0)$ is rational. Conversly, if a line through $(-1, 0)$ with rational slope intersects the circle at another point (u_0, v_0), then u_0 and v_0 are rational.

Let t be a rational number. Let us consider the line with slope t through $(-1, 0)$ and it has the equation $\frac{v-0}{u+1} = t$ or $v = t(u+1)$. Substituting this in (2.10) we obtain $u^2 + t^2(u+1)^2 = 1$ or $u^2(1+t^2) + 2t^2u + t^2 - 1 = 0$. Now we can use the quadratic formula to solve for u, or we observe that one root is -1 and the sum of the roots of the equation $au^2 + bu + c = 0$ is $-\frac{b}{a}$, hence

$$u - 1 = -\frac{2t^2}{1+t^2}$$

or

$$u = \frac{1-t^2}{1+t^2}$$

Let $t = \frac{s}{r}$ with $(s, r) = 1$ and so

$$u = \frac{x}{z} = \frac{1-\frac{s^2}{r^2}}{1+\frac{s^2}{r^2}} = \frac{r^2-s^2}{r^2+s^2}$$

Since $(x, z) = 1$ and if $(r^2 - s^2, r^2 + s^2) = 1$, then

$$x = r^2 - s^2, z = r^2 + s^2, y = 2rs$$

But $(r^2 - s^2, r^2 + s^2) \neq 1$, we cannot take $x = r^2 - s^2, z = r^2 + s^2$, because $(r, s) = 1$ implies that $(r^2 - s^2, r^2 + s^2) = 1, 2$. Again if $(r^2 - s^2, r^2 + s^2) = 2$, then

$$x = \frac{r^2-s^2}{2}, z = \frac{r^2+s^2}{2}, y = rs$$

This equation can be written as the form stated in the theorem. Here both r and s must be odd, so we can transform

$$z = (\frac{r+s}{2})^2 + (\frac{r-s}{2})^2$$

$$x = (\frac{r+s}{2})^2 - (\frac{r-s}{2})^2$$

$$y = 2(\frac{r+s}{2})(\frac{r-s}{2})$$

Now letting $m = \frac{r+s}{2}$ and $n = \frac{r-s}{2}$ and adding switching x and y, we see that the solution is again of the form

$$x = m^2 - n^2, y = 2mn, z = m^2 + n^2$$

Conversely, we can easily verify that for any $(m, n) = 1$, these formulas yield a Pythagorean triple.

CHAPTER 3

Pell's equation

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 $17th$ 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 from 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 $x = \frac{2ab}{2} = ab, y = \frac{2b^2-2}{2} = b^2 - 1$ 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 $k = \pm1, \pm2, \pm4$, 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 $83 \cdot 1^2 - 2 = 9^2$

So applying above method $x = \frac{2ab}{k}$, $y = \frac{b^2+na^2}{k}$ is a solution to (3.6), i.e, $x = \frac{2\times9}{2}, y = \frac{81+83\times1}{2}$ 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 $n \cdot 1^2 + (m^2 - n) = m^2$.

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 choosen so that so that $am+b$ is divisible by k then $m^2 - n$ and $bm + na$ are also divisible by k with such choice of m 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 $k = \pm 1, \pm 2, \pm 4$ 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 $\mathbb{Z}[\sqrt{d}]$
The continued fraction expansion of $\sqrt{d}$ is given by the following algorithm:See([4])

1. The continued fraction has the form $[a_0, \overline{a_1, a_2 \cdots a_2, a_1, 2a_0}]$.

2. The expansion of $\sqrt{d}$ is computed by

$$A_0 = 0 \quad B_0 = 1 \quad a_k = \lfloor \frac{A_k + \sqrt{d}}{B_k} \rfloor$$

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

3. The convergents $\frac{p_k}{qk}$ of $\sqrt{d}$ satisfy

$$p_k^2 - dq_k^2 = (-1)^{k+1} B_{k+1}$$

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

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

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

also the conjugate of $\alpha = a+b\sqrt{d}$ is $\overline{\alpha} = a-b\sqrt{d}$ 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

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

Dividing by q, we get

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

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

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

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 kth 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 $j \geq 0$. 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 infinetly 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 $m \mid k$. Then we have $k = jm$ and substituting in 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 convergents $\frac{p_{jm-1}}{q_{jm-1}}$ 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 $\sqrt{19}$.

$$\frac{A_0 + \sqrt{19}}{B_0}, \quad A_0 = 0, B_0 = 1$$
$$A_{k+1} = a_k B_k - A_k, \quad B_{k+1} = \frac{(n - (A_{k+1})^2)}{Bk}$$
$$x_k = \frac{A_k + \sqrt{n}}{B_k}, \quad a_k = [x_k]$$

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 $\frac{p_5}{q_5} = \frac{170}{39}$, so

$$19 \cdot 39^2 + 1 = 170^2$$

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

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

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}) gives 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
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.

BIBLIOGRAPHY

1. Apostol T.M., "*Introduction to Analytic Number Theory*" , Spinger International Student Edition,Narosa Publishing House (1989)

2. Burton D.M."*Elementary Number Theory*" , Tata McGraw-Hill Edition, Sixth Edition (2006)

3. Hardy G.H.,Wright E.M."*An Introduction to the Theory of Numbers*" Oxford Science Publications, Fifth Edition (1979)

4. Kumundury R,Romero C., "*Number Theory with Computer Application*" Prentice hall (1998)

5. Mapa S.K."*Higher Algebra*" , Milinda De for Levant Books, Sixth Revised Edition (2004)