Study on Diophantine Equations

A Dissertation for

MAT-651 Discipline Specific Dissertation

Credits: 16

Submitted in partial fulfilment of Masters Degree

M.Sc. in Mathematics

by

Mr. ELISEUS MORAES

22P0410009

ABC ID : 8840104659724

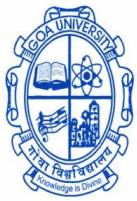
201911555

Under the Supervisor of

Dr. MANVENDRA TAMBA

School of Physical & Applied Sciences

Mathematics Discipline



GOA UNIVERSITY

APRIL 2024

Examined by: Seal of the School

DECLARATION BY STUDENT

I hereby declare that the data presented in this Dissertation report entitled, "Study on Diophantine Equations" is based on the results of investigations carried out by me in the Mathematics Discipline at the School of Physical & Applied Sciences, Goa University under the Supervision of Dr. Manvendra Tamba and the same has not been submitted elsewhere for the award of a degree or diploma by me. Further, I understand that Goa University will not be responsible for the correctness of observations / experimental or other findings given the dissertation.

I hereby authorize the University authorities to upload this dissertation on the dissertation repository or anywhere else as the UGC regulations demand and make it available to any one as needed.

Signature: Moraes

Student Name: Eliseus Moraes

Seat no: 22P0410009

Date: 09/05/2024

Place: GOA UNIVERSITY

COMPLETION CERTIFICATE

This is to certify that the dissertation report "Study on Diophantine Equations" is a bonafide work carried out by Mr. Eliseus Moraes under my supervision in partial fulfilment of the requirements for the award of the degree of Master of Science in Mathematics in the Discipline Mathematics at the School of Physical & Applied Sciences , Goa University.

Signature : _____

Supervisor : Dr. Manvendra Tamba

Date: 09/05/2024

Signature of HoD of the Dept

Date: 10/05/2024

Place: Goa University

School of Physical and Applied Sciences Goa University

School Stamp

PREFACE

This Project Report has been prepared in partial fulfilment of the requirement for the Subject: MAT - 651 Discipline Specific Dissertation of the programme M.Sc. in Mathematics in the academic year 2023-2024.

The topic assigned for the research report is: " Study on Diophantine Equations." This survey is divided into five chapters. Each chapter has its own relevance and importance. The chapters are divided and defined in a logical, systematic and scientific manner to cover every nook and corner of the topic.

FIRST CHAPTER :

This is an introductory part which gives the origin and brief idea about Diophantine equations, (see [4]).

SECOND CHAPTER:

This chapter is based on Quadratic Diophantine equations (see [7]). We will look at the results involving its solutions. In the beginning we discuss about Pythagorean triples. further we look at Quadratic Diophantine equations related to Pythagorean triples and lastly we talk about the equation $ax^2 + by^2 + cz^2 = 0$, .

THIRD CHAPTER:

In this chapter deals with Linear Diophantine equations with 2 or more variables (see [5]). Firstly we look at equations with 2 variables and learn about conditions for having solutions & also how to deduce more solutions from one. Next we will look at equations with more than 2 variables, we will learn how to reduce this equation in terms of 2

variables and hence find its solutions.

FOURTH CHAPTER:

In this chapter we look at a special kind of Diophantine equation called *Pell's equation* (see [2]). In this topic we discuss about Quadratic Surds and its properties and Existence of rational solution of Pell's equation. Further we look at Power Of Solution and Chebyshev polynomial. Lastly we use above topics for Related pell's equation.

FIFTH CHAPTER:

This chapter entirely based on research articles about Exponential Diophantine Equations. There are 5 sections in this chapter and each section contains 1 article. Following articles are reviewed [1], [8], [3], [6], [9].

ACKNOWLEDGEMENTS

First and foremost, I would like to express my gratitude to my Mentor, Dr. Manvendra Tamba, who was a continual source of inspiration. He pushed me to think imaginatively and urged me to do this homework without hesitation. His vast knowledge, extensive experience, and professional competence in Number Theory enabled me to successfully accomplish this project. This endeavour would not have been possible without his help and supervision. Also I would like to thank all the faculties of the mathematics discipline, programme director Dr. Mailattu Kunhanandan and dean of the school Prof. Ramesh V.Pai for giving me this opportunity to do this project.

ABSTRACT

In mathematics, a Diophantine equation is an equation, typically a polynomial equation in two or more unknowns with integer coefficients, for which only integer solutions are of interest. The purpose of this report is to analyse different types of Diophantine equation and determine it's solutions if it exists. We will also learn the conditions for existence of solutions and ways to obtain it.

Furthermore, we will look at some research articles involving exponential Diophantine equations and determine its solutions. Authors make use of *Catalan's conjecture* but in present report, we find solutions without making use of this result. Also in final article, author A. Suvarnamani in [9] claimed that diophantine equation $p^x + (p+1)^y = z^2$ has a unique solution for a prime p and $x, y, z \in \mathbb{N} \bigcup \{0\}$ but we show that it has more non-negative solutions.

KEY WORDS:

Diophantine equation, Pythagorean triples, Pell's Equation, Quadratic surds, Chebyshev polynomial, Twin primes, Twin prime conjecture, Mersenne Prime.

Table of contents

Notations and Abbreviations

$\mathbb{N}$	Set of Natural numbers
$\mathbb{Z}$	Set of Integers
$\mathbb{Q}$	Set of Rational numbers
$(x,y)=d$	d is $g.c.d$ of x & y
$a\|b$	a divides b

Chapter 1

INTRODUCTION

All information in this section are taken from [4].
The first exposition of Diophantine equations, as simply equation to solve was due to Diophantus of Alexandria. To solve Diophantine equation means to solve an equation whose only solutions of interest are integers.

Let $x_1, x_2, \ldots, x_n$ be n variables & let $f(x_1, x_2, \ldots, x_n)$ be polynomial in these variables with rational coefficients. W.l.o.g suppose that the coefficients are integers since we shall be concerned with equations $f(x_1, x_2, \ldots, x_n) = 0$, An obvious question is to find solutions **or** all the solutions of $f(x_1, x_2, \ldots, x_n) = 0$ in,

1. rational numbers *i.e in the field* $\mathbb{Q}$
2. rational integers *i.e in the ring* $\mathbb{Z}$

Suppose that $f(x_1, x_2, \ldots, x_n) = 0$ is a homogeneous polynomial. Leaving aside the trivial solution $x_i = 0$, $\forall i \in \{1, 2, \ldots, n\}$, we can confine ourselves in finding integer

solution with $(x_1, x_2, \ldots, x_n) = 1$.

Suppose if $f(x_1, x_2, \ldots, x_n) = 0$ is non-homogeneous polynomial. We let

$$x_1 = \frac{y_1}{y_{n+1}}, x_2 = \frac{y_2}{y_{n+1}}, \ldots, x_n = \frac{y_n}{y_{n+1}} \qquad y_i \in \mathbb{Z}$$

Giving us a homogeneous equation,

$$g(y_1, y_2, \ldots, y_n, y_{n+1}) = 0$$

There is now one to one correspondence between the rationals values $x_1, x_2, \ldots, x_n$ and those integer values $y_1, y_2, \ldots, y_n, y_{n+1}$ with $y_{n+1} \neq 0$ and $(y_1, y_2, \ldots, y_n, y_{n+1}) = 1$.

More generally, we may impose restrictions on variables, like we are suppose to find only non-negative integer solutions. We may also say that we are interested in finding prime solution.

Given any Diophantine equation, number of questions may arise like, Are there solutions to the equation? Can we deduce more solutions when we are given one of the solution? What can be said about the number of solutions?

Chapter 2

QUADRATIC DIOPHANTINE EQUATIONS

All the material in this chapter is taken from [7].

For a function $f(x_1, x_2, \ldots, x_m)$ of m variables $x_1, x_2, \ldots, x_m$; the Diophantine equation can be considered in two primary ways,

1. $f(x_1, x_2, \ldots, x_m) = 0$

or

2. $f(x_1, x_2, \ldots, x_m) = N$

where N is an integer & we are supposed to find solution in integers for $x_1, x_2, \ldots, x_m$ of the equation.

First one is special case of the second one but we prefer to separate it since one uses different techniques for two cases.

2.1 Pythagorean triples

one of the first Diophantine to be solved was to find integer sides of right triangles. By the theorem of Pythagoras, if x and y are lengths of the legs and z is the length of the hypotenuse, then

$$x^2 + y^2 = z^2 \text{———(1)}$$

If x,y,z in (1) are positive integers, then x,y,z are said to be pythagorean triples. the solution is said to have primitive solution if (x,y,z)=1.

Theorem 2.1.0.1. *All primitive solutions of (1) with $x, y, z \in \mathbb{Z}$ are given by,*
$x = u^2 - v^2$, $y = 2uv$ & $z = u^2 + v^2$, where $u > v > 0$, $(u, v) = 1$ and u & v are of opposite parity, $u, v \in \mathbb{Z}$.

Proof:

Note that if any two of the x,y or z have a common factor then it must also divide the third.

Thus if (x,y,z)=1 then (x,y)=(x,z)=(y,z)=1

Also, if x & y are both odd then $x^2 + y^2 \equiv 2(mod 4)$

this cannot be the square of an integer.

Thus z is odd & one of x & y, say y is even while x is odd.

$\therefore y = 2y_1 \qquad , y_1 \in \mathbb{Z}$

$\therefore (1) \implies y^2 = 4y_1^2 = z^2 - x^2$

$\implies y_1^2 = (\frac{z-x}{2})(\frac{z+x}{2})$ ———(a)

since $(\frac{z-x}{2}, \frac{z+x}{2}) = 1$, we see unique factorisation that $\exists u, v \in \mathbb{Z}$ such that $u > v > 0$, $(u, v) = 0$.

Let $\frac{z+x}{2} = u^2$ and $\frac{z-x}{2} = v^2$,

$$u^2 + v^2 = \frac{z+x}{2} + \frac{z-x}{2}$$
$$= z \leftarrow odd$$

$\therefore$ one of the u or v must be odd & other must be even.

finally,

$z = u^2 + v^2$

$x = u^2 - v^2$ $\{u^2 - v^2 = \frac{z+x}{2} - \frac{z-x}{2} = x\}$

& $y = 2y_1 = 2uv$ {from (a)}

Corollary 2.1.0.2. *All Pythagorean triplets are given by,*

$x = k(u^2 - v^2)$, $y = 2kuv$, $z = k(u^2 + v^2)$

where $k \in \mathbb{N}$ and u & v are as in thm 2.1.0.1

We have a short table of primitive Pythagorean triangles.

u	**v**	**x**	**y**	**z**
2	1	3	4	5
3	2	5	12	13
4	1	15	8	17
4	3	7	24	25
5	2	21	20	29

u	**v**	**x**	**y**	**z**
5	4	9	40	41
6	1	35	12	37
6	5	11	60	61
7	2	45	28	53
7	4	33	56	65

Theorem 2.1.0.3. *There does not exist a primitive pythagorean triangles with atleast two sides being squares.*

Proof:

There are two cases to consider,

case 01: $x^4+y^4=z^2$——(A)

w.l.o.g assume that $(x,y,z)=1$ be the pythagorean triangle with the least primitive z.

by thm 2.1.0.1,

$x=u^2-v^2, \qquad y=2uv, \qquad z=u^2+v^2$

where $(u,v)=1$, $u>v>0$ and u & v are of opposite parity.

If u is even & v is odd then,

$$\begin{aligned} x^2 &\equiv (u^2-v^2)(mod4) \\ &\equiv [u^2(mod4)-v^2(mod4)](mod4) \\ &\equiv (0-1)(mod4) \\ &\equiv -1(mod4) \\ &\equiv 3(mod4) \end{aligned}$$

this is contradiction since for $a\in\mathbb{Z}$

$$\begin{aligned} a^2 =&\{0(mod4), even"a" \\ &\{1(mod4), odd"a" \end{aligned}$$

$\therefore$ u is odd.

so the in eqn,

$y^2=2uv$

we must have to occour to even power on the R.H.S,

thus $u = u_0^2$ and $v = 2v_0^2$,where $u_0, v_0 \in \mathbb{N}$

$\therefore x^2 = u_0^4 - 4v_0^4$

i.e $x^2 + (2v_0^2)^2(u_0^2)^2$

Now, $(u_0, 2v_0) = 1$, thus by Thm 2.1.0.1. we have,

$u_0^2 = t^2 + w^2$ & $v_0^2 = tw$,where $(t,w) = 1$

thus t= α^2 & $w = \beta^2$

$\implies u_0^2 = \alpha^4 + \beta^4$

$\therefore$ we have,

$u_0^2 = u \leq u^2 < z \leq z^2$

$\implies 0 < u_0 < z$

this is contradiction as we choose z to be least satisfying (A).

case 02: $x^2 + y^4 = z^4$——(B)

w.l.o.g assume that $(x,y,z) = 1$ be the pythagorean triangle with the least primitive z

if x is even, then by Thm 2.1.0.1,

$\exists\ (m,n) = 1, m > n > 0$ such that $x = 2mn$, $y^2 = m^2 - n^2$ and $Z62 = m^2 + n^2 \implies z^2 > m^2$

$\therefore (yz)^2 = m^4 - n^4$

$\implies n^4 + (yz)^2 = m^4$

this contradiction to minimality of z.

if x is odd, then

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

if suppose $(z^2 - y^2, z^2 + y^2) = p$, for prime p

then $p|(z^2 - y^2)$ & $p|(z^2 + y^2)$

$\implies z^2 - y^2 = pa$ and $z^2 + y^2 = pb$

$\implies 2z^2 = p(a+b)$ and $2y^2 = p(b-a)$

$p \neq 2$ as y & z are of opposite parity.

$\implies p|z^2$ and $p|y^2$

$\implies (z,y) = 1$

this is contradiction as $(x,y,z) = 1 \implies (x,y) = (x,z) = (y,z) = 1$

$\therefore (z^2 - y^2, z^2 + y^2) = 1$

Thus $\exists\ r,s \in \mathbb{Z}$ with $(r,s) = 1$, $s > r$ such that,

$z^2 - y^2 = r^2$ and $z^2 + y^2 = s^2$

$\therefore 2z^2 = r^2 + s^2$ and $2y^2 = s^2 - r^2$

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

if suppose $(\frac{s+r}{2}, \frac{s-r}{2}) = d$, $d > 1$

$\implies \frac{s+r}{2} = da$ and $\frac{s-r}{2} = db \implies s = d(a+b)$ and $r = d(b-a)$

$\implies d|s$ and $d|r$ This is contradiction, since $(z^2 - y^2, z^2 + y^2) = (r^2, s^2) = 1$

$\therefore (\frac{s+r}{2}, \frac{s-r}{2}) = 1$

$\therefore$ by Thm 2.1.0.1,

$\exists m,n \in \mathbb{Z}$ of opposite parity such that,

$\frac{s+r}{2} = m^2 - n^2$, $\frac{s-r}{2} = 2mn$ & $z = m^2 + n^2$

or

$\frac{s-r}{2} = m^2 - n^2$, $\frac{s+r}{2} = 2mn$ & $z = m^2 + n^2$

In both cases,

$s^2 - r^2 = 8mn(m^2 - n^2)$

$\implies 2y = 8mn(m^2 - n^2)$

since y is even, let $y = 2y_1$

$\therefore 2(2y_1) = 8mn(m^2 - n^2)$

$\implies y_1 = mn(m^2 - n^2) = mn(m-n)(m+n)$

since (m,n)=1 & are of opposite parity we have (m-n,m+n)=1.

Also,

$(m, m+n) = (m, m-n) = (n, m+n) = (n, m-n) = 1$

Thus $\exists$ a positive integers k, w, p, q such that,

$m = k^2, \qquad n = w^2, \qquad m-n = p^2, \qquad m+n = q^2$

Thus, $p^2.q^2 = (m-n)(m+n)$

$\implies (pq)^2 = m^2 - n^2 = k^4 - w^4$

$\implies (pq)^2 + w^4 = k^4$

since $k^4 < m^2 < m^2 + n^2 = z < z^4$, we have $k < z$

THis contradicts the minimality of z

Corollary 2.1.0.4. *There does not exist a pair of pythagorean triplets such that a leg & hypothenuse of one are the legs of the other.*

Proof:

suppose to the contraray $\exists$ pythagorean triplets such that

$x^2 + y^2 = z^2 \qquad \& \qquad x^2 + z^2 = u^2$

$\implies y^2 = z^2 - x^2$

$\therefore y^2u^2 = (z^2 - x^2)(z^2 + x^2)$

$\implies (yu)^2 = z^4 - x^4$

$\implies x^4 + (yu)^2 = z^4$

This contradicts Thm 2.1.0.2

$\therefore$ such triplets does not exist.

EXERCISE

Q1: Find all primitive pythagorean triangles that have one of legs & hypotenuse differing by a fixed positive integer k.

Soln:

w.l.o.g let $(x,y,z) = 1$, where x is odd, y is even & z is hypotenuse.

Case 01: If k is odd.

Then hypotenuse and even leg must differ by k.

Thus we have,

$z = y + k$

$\implies u^2 + v^2 = 2uv + k$

$\implies k = (u-v)^2$

Thus, if there are primitive solutions then k must be a square, i.e $k = q^2$, for $q \in \mathbb{N}$

and $\because u > v$ we have u=v+q

$\therefore$ The solutions are given by,

$$\begin{aligned} x &= u^2 - v^2 \\ &= (u-v)(u+v) \\ &= q(2v+q) \\ y &= 2uv \\ &= 2v(q+v) \end{aligned}$$

$$\begin{aligned} z &= u^2+v^2 \\ &= v^2+q^2+2vq+v^2 \\ &= 2v^2+q^2+2vq \end{aligned}$$

where $v,q>0$ & are of opposite parity.

In particular, if $q=1$ then k=1 &

$x=2v \qquad , y=2v(v+1) \qquad \& \qquad z=2v^2+2v+1$

Case 02: If k is even.

Then hypotenuse and odd leg must differ by k.

Thus we have,

i.e $z=x+k$

$\implies u^2+v^2=u^2-v^2+k$

$\implies k=2v^2$

Thus problem has a solution if $k=2p^2 \qquad p\in\mathbb{Z}$

$\therefore v=p$ & u is arbitrary such that $u>p$ & of opposite parity,

Thus,

$$\begin{aligned} x &= u^2-v^2 \\ &= u^2-p^2 \\ y &= 2uv \\ &= 2up \\ z &= u^2+v^2 \\ &= u^2+p^2 \end{aligned}$$

In particular, for k=2 we have,

$x=u^2-1 \qquad , y=2u \qquad \& \qquad z=u^2+1$

When u is even & $u>2$, this can also be written as,

$x=4w^2-1 \qquad , y=4w \qquad \& \qquad z=4w^2+1$

Q2: Find all the Pythagorean triangles whose sides are in an arithmetic progression.

Soln:

Pythagorean triangles are given by,

$$x^2+y^2=z^2$$

we want a Pythagorean triangle whose sides are arithmetic progression. So we want sides whose common difference is k, for $k \in \mathbb{Z}$

i.e $(x-k)^2+x^2=(x+k)^2$

$\implies x^2+k^2-2kx+x^2=x^2+k^2+2kx$

$\implies x^2=4kx$

$\implies x=4k$

$\therefore$ Our triangles are given by $(x,y,z)=(3k,4k,5k)$.

Q3: Find all primitive Pythagorean triangles in which one of the sides is a square.

Soln:

Given Pythagorean triangle $x^2+y^2=z^2$, $\{x$ is odd side, y is even side and z is hypotenuse$\}$ there are three cases depending on which sides is to be a square.

Case 01: The hypotenuse is to be a square.

$x^2+y^2=(z^2)^2=z^4$

we have,

$x=u^2-v^2, \quad y=2uv \quad \& \quad z^2=u^2+v^2$

where $(u,v)=1$, $u>v>0$ & are of opposite parity.

Then,

$u=2mn, \quad v=m^2-n^2 \quad \& \quad z=m^2+n^2$

. or

$u=m^2-n^2, \quad v=2mn \quad \& \quad z=m^2+n^2$

where $(m,n) = 1$, $m > n > 0$ & are of opposite parity.

$\therefore x = |m^4 + n^4 - 6m^2n^2|, \quad y = 4mn(m^2 - n^2) \quad \& \quad z = m^2 + n^2$

Case 02: The odd leg is to be a square.

Then, $x^4 + y^2 = z^2$

$\therefore x^2 = u^2 - v^2$

or $x^2 + v^2 = u^2$

where $u > v$, $(u,v) = 1$ and are of opposite parity.

Here u must be odd & v must be even $\because x$ is odd.

Thus,

$x = m^2 - n^2 \quad , v = 2mn \quad \& \quad u = m^2 + n^2$

where $(m,n) = 1 \quad m > n > 0 \quad$ & are of opposite parity.

Thus we have,

$x = m^2 - n^2 \quad , y = 4mn(m^2 + n^2) \quad \& \quad z = m^4 + n^4 + 6m^2n^2$

Case 3: The even leg to be square,

Then, $x^2 + y^4 = z^2$

$\therefore y^2 2uv$

Here $(u,v) = 1$ & are of opposite parity.

Also y is even i.e $y = 2w \quad , w \in \mathbb{Z}$

$\implies 4w^2 = 2uv$

$\implies 2w^2 = uv$

Thus,

$x = |m^4 - 4n^4| \quad ,y = 2mn \quad \& \quad z = m^4 + n^4.$

Q4: Prove that $\nexists$ a Pythagorean triangle with a square area.

Soln:

Given that,

$\frac{1}{2}xy = n^2$

T.S.T: Pythagorean triplets of such triangles does not exist.

w.l.o.g let $(x,y,z) = 1$, where x is odd & y is even. Suppose $\exists$ such triangles

i,e $x^2 + y^2 = z^2$

$\implies x^2 + (\frac{2n^2}{x})^2 = z^2$

$\implies x^4 + (2n^2)^2 = (zx)^2$

where $(u,v) = 1$, $u > v > 0$ & are of opposite parity.

$2n^2 = 2uv$,$x^2 = u^2 - v^2$ & $zx = u^2 + v^2$.

$\implies n^2 = 2uv$

$\therefore u = u_0$ & $v = v_0$

$\therefore x^2 = u^2 - v^2 \implies x^2 = u_0^4 - v_0^4$

This is contradiction as $\nexists$ Pythagorean triangles whose 2 sides are squares.

Q5: Solve $x^2 + (2y)^4 = z^2$ in positive integers.

Soln:

w.l.o.g let (x,y,z)=1

Here we notice that $2x$ is even $\therefore y$ must be odd.

Thus,

$x = u^2 - v^2$,$(2y)^2 = 2uv$ & $z = u^2 + v^2$.

where $(u,v) = 1$, $u > v > 0$ & are of opposite parity.

$\therefore (2y)^2 = 2uv$

$\implies 2y^2 = uv$

$\therefore u = \alpha^2 \quad \& \quad v = 2\beta^2$

. or

$u = 2\beta^2 \quad \& \quad v = \alpha^2$

Considering either cases,

$x = |\alpha^2 - 2\beta^2| \quad , y = \alpha\beta \quad \& \quad z = \alpha^2 + 2\beta^2$

Q6: Solve $(2x)^2 + y^4 = z^2$ in positive integers.

Soln:

w.l.o.g let (x,y,z)=1

Here we notice that $2y$ is even $\therefore x$ must be odd.

Thus,

$2x = 2uv \quad , y^2 = u^2 - v^2 \quad \& \quad z = u^2 + v^2.$

where $(u,v) = 1$, $u > v > 0$ & are of opposite parity.

$y^2 = u^2 - v^2$ can be written as $y^2 + v^2 = u^2$

$\because y$ is odd & u and v are of opposite parity v must be even.

$\therefore y = \alpha^2 - \beta^2 \quad , v = 2\alpha\beta \quad \& \quad u = \alpha^2 + \beta^2$

where $(\alpha,\beta) = 1$, $\alpha > \beta > 0$ & are of opposite parity.

Thus we have,

$x = 2\alpha\beta(\alpha^2 + \beta^2)$

$y = \alpha^2 - \beta^2$

$z = 2\alpha^4 - 2\beta^4$

Q7: If (x,y,z) are primitive Pythagorean triples, then hypotenuse can never extend a leg by 4.

Soln:

$\because (x,y,z) = 1$, one leg and hypotenuse is odd and other is even, say x is odd and y is even.

$\therefore$ hypotenuse exceeds odd leg by 4.

i.e $x^2 + y^2 = (x+4)^2$

$\implies x^2 + y^2 = x^2 + 16 + 8x$

$\implies y^2 = 16 + 8x$

$\implies y^2 - 4^2 = 8x$

$\implies (y-4)(y+4) = 8x$

$\implies (2m-4)(2m+4) = 8x$ {y=2m $\because$ y is even.}

$\implies (m-4)(m+4) = 2x$

if m is odd, then L.H.S is odd & R.H.S is even.

if m is even, then L.H.S is divisible by 4 & R.H.S is only divisible by 2 as x is odd.

2.2 Quadratic Diophantine equations related to Pythagorean triples

Theorem 2.2.0.1. *The solution in the positive integers of,*

$x^2 + 2y^2 = z^2$, *(x,y,z)=1 is given by,*

$x = |u^2 - 2v^2|$ $,y = 2uv$ $\& \; z = u^2 + 2v^2$ *where* $u, v > 0$ & $(u, 2v) = 1$.

Proof:

If $(x,y,z) = 1$, then we see that we must have x(& so z) odd.

Considering congruence modulo 4 we see that,

$x^2 \equiv 1(mod4)$ & $z^2 \equiv 1(mod4)$

$\therefore 2y^2 = z^2 - x^2 \equiv 0(mod4)$

$\implies y^2 \equiv 0mod4$

hence y is even.

let $y = 2w$ then we have,

$x^2 + 2(2w)^2 = z^2$

$\implies 8w^2 = z^2 - x^2$

$\implies 2w^2 = (\frac{z+x}{2})(\frac{z-x}{2})$ ——-(a)

& $since(\frac{z+x}{2}, \frac{z-x}{2}) = 1$, we must have, by unique factorisation

$\frac{z+x}{2} = u^2$ & $\frac{z-x}{2} = 2v^2$

. or ——-(b)

$\frac{z+x}{2} = 2v^2$ & $\frac{z-x}{2} = u^2$

In (b), i we subtract equations in either case we get,

$x = u^2 - 2v^2$ or $x = 2v^2 - u^2$

$x = |u^2 - 2v^2|$

If we add equations in either cases we get,

$z = u^2 + 2v^2$

And (a) becomes,

$2w^2 = u^2(2v^2)$

$\implies 4w^2 = 4u^2v^2$

$\implies 2w = 2uv$ {taking positive roots}

$\implies y = 2uv$

Theorem 2.2.0.2. *The solution in relative prime positive integers of* $x^2 + y^2 = 2z^2$ *is given by,*

$x = u^2 - v^2 + 2uv$,$y = |u^2 - v^2 - 2uv|$ & $z = |u^2 + v^2|$

where $u, v \in \mathbb{Z}$, $(u, v) = 1$ *& are of opposite parity.*

Proof:

Since x,y & z are relatively prime, we can see that none of them can be even.

i.e x&y are both odd, $x^2 + y^2 = 2z^2$

$\therefore x^2 \equiv 1(mod4)$ & $y^2 \equiv 1(mod4)$

$x^2 + y^2 \equiv 2(mod4)$

$2z^2 \equiv 2(mod4)$

$z^2 \equiv 1(mod4)$ $\therefore$ z is odd.

Now, since x&y are both odd

$\implies \frac{x+y}{2}$ & $\frac{x-y}{2}$ are both integers & so,

$(\frac{x+y}{2})^2 + (\frac{x-y}{2})^2 = z^2$——-(a)

If $x = y$, then

$x = y = z = 1$ is a primitive solution.

otherwise,

we apply Thm 2.1.0.1 to eqn (a),

$\frac{x+y}{2} = u^2 - v^2$, $\frac{x-y}{2} = 2uv$ & $z = u^2 + v^2$

. or ——(b)

$\frac{x+y}{2} = 2uv$, $\frac{x-y}{2} = u^2 - v^2$ & $z = u^2 + v^2$

In either cases,

$z = u^2 + v^2$

solving the other two equations in (b) we get,

$x = u^2 - v^2 + 2uv$ & $y = |u^2 - v^2 - 2uv|$

Theorem 2.2.0.3. *All solutions of,* $x^2 + y^2 + z^2 = t^2$; *where y&z are even are given by,*

$$x = \frac{p^2 + q^2 - r^2}{2}; \qquad y = 2p, \qquad z = 2q \qquad \& \qquad t = \frac{p^2 + q^2 + r^2}{2}.$$

where p&q are positive integers & r runs through the divisors of $p^2 + q^2$ *less than* $\sqrt{p^2 + q^2}$

Proof:

suppose x, y, z are odd,

$\implies x^2 \equiv 1(mod 4), \qquad y^2 \equiv 1(mod 4), \qquad z^2 \equiv 1(mod 4).$

$\implies t^2 = x^2 + y^2 + z^2 \equiv 3(mod 4)$,which is not true.

suppose only 1 were even say x is even then,

$\implies x^2 \equiv 0(mod 4), \qquad y^2 \equiv 1(mod 4), \qquad z^2 \equiv 1(mod 4).$

$\implies t^2 = x^2 + y^2 + z^2 \equiv 2(mod 4)$,which is not true.

Thus two of $x, \&, z$ must be even,

say $y = 2p$ & $z = 2q$ $; p, q \in \mathbb{Z}$

let $t-x=u$ then,

$(x+u)^2 = x^2+4p^2+4q^2$

$\implies x^2+u^2+2xu = x^2+4p^2+4q^2$

$\implies u^2 = 4p^2+4q^2-2xu$

Thus u is even, say $u=2r$,

$\therefore 4r^2 = 4p^2+4q^2-4xr$

$\implies r^2 = p^2+q^2-xr$

$\implies xr = p^2+q^2-r^2$

Thus $r|p^2+q^2$

$\therefore x = \frac{p^2+q^2-r^2}{2} \in \mathbb{Z}$

$$\begin{aligned} \&t &= u+x \\ &= 2r+\tfrac{p^2+q^2-r^2}{2} \\ &= \tfrac{p^2+q^2+r^2}{2} \in \mathbb{Z} \end{aligned}$$

And since we want x to be positive,

$p^2+q^2-r^2 > 0$

$\implies p^2+q^2 > r^2$

$\implies r^2 < \sqrt{p^2+q^2}$

EXERCISE:

Q1: Solve $x^2+3y^2=z^2$, in positive integers.

Soln:

w.l.o.g let (x,y,z) be primitive solutions. i.e $(x,y,z)=1$.

Case 01: If x is odd & y is even, then

$$\begin{aligned} z^2 &\equiv (1+3\times 0) \mod 4 \\ &\equiv 1 \mod 4 \end{aligned}$$

$\therefore z$ is odd.

$$\begin{aligned}
&\therefore 3y^2 = z^2 - x^2 \\
&\implies 3(2w)^2 = (z-x)(z+x) \\
&\implies 3w^2 = \left(\frac{z-x}{2}\right)\left(\frac{z+x}{2}\right)
\end{aligned}$$

We know that $\left(\frac{z-x}{2}\right)\left(\frac{z+x}{2}\right) = 1$

$\therefore$ We must have unique factorisation,

$$\frac{z+x}{2} = u^2 \quad \& \quad \frac{z-x}{2} = 3v^2$$

or

$$\frac{z+x}{2} = 3v^2 \quad \& \quad \frac{z-x}{2} = u^2$$

where $(u, 3v) = 1$

If we add equations above in either case we get,

$z = u^2 + 3v^2$

If we subtract equations in either case we get,

$x = u^2 - 3v^2$ or $x = 3v^2 - u^2$

$\implies x = |u^2 - 3v^2|$

Also,

$$3w^2 = \left(\frac{z-x}{2}\right)\left(\frac{z+x}{2}\right) \quad .$$
$$\implies 3w^2 = 3u^2v^2$$
$$\therefore 3y^2 = 3(2w)^2 = 12u^2v^2$$
$$\implies y = 2uv$$

$\therefore$ Solutions in positive integers are of the form,

$x = |u^2 - 3v^2|$, $y = 2uv$ & $z = u^2 + 3v^2$

Case 02: If x is even & y is odd, then

$$z^2 \equiv (0 + 3 \times 1) \mod 4$$
$$\equiv 3 \mod 4$$
$$\equiv -1 \mod 4$$

This is impossible.

Q2: Solve $x^2 + 2y^2 = z^4$.

Soln:

The equation can be written in the form,

$$x^2 + 2y^2 = (z^2)^2$$

w.l.o.g let $(x, y, z) = 1$

$\therefore \exists\, u, v \in \mathbb{Z}^+$, $(u, v) = 1$ & are of opposite parity such that

$$x = |u^2 - 2v^2|, \quad y = 2uv \quad \& \quad z^2 = u^2 + 2v^2$$

Now for $z^2=u^2+2v^2$

$\therefore \exists\, m,n \in \mathbb{Z}^+$, $(m,n)=1$ & are of opposite parity such that

$$u=|m^2-2n^2|, \quad v=2mn \quad \& \quad z=m^2+2n^2$$

$\therefore$The solution in positive integers are given by,

$$x=|m^4+n^4-8m^2n^2|, \quad y=4m^2n^2(|m^2-2n^2|) \quad \& \quad z=m^2+2n^2$$

2.3 The equation $ax^2+by^2+cz^2=0$

In this section we make use of following two lemmas which deal with certain types of congruence equations to prove the main theorem. This proof also gives bound for a solution, if there is one;

Lemma 2.3.0.1. *Let λ,μ,ν be positive real numbers with product $\lambda\mu\nu=m$ an integer, then any congruence $\alpha x+\beta y+\gamma z\equiv 0(modm)$ has a solution x,y,z not all zero, such that $|x|\leq\lambda$, $|y|\leq\mu$ & $|z|\leq\gamma$.*

Proof:

Let x range over the values 0,1,2, ...,[λ], y range over the values 0,1,2, ...,[μ] & z range over the values 0,1,2, ...,[ν].

This gives us,

(1+[λ])(1+[μ])(1+[ν])=$\lambda\mu\nu > m$, different triples (x,y,z).

Thus there must be at least two distinct triples (x_1,y_1,z_1) & (x_2,y_2,z_2) such that,

$\alpha x_1+\beta y_1+\gamma z_1 \equiv 0(modm) \qquad \& \qquad \alpha x_2+\beta y_2+\gamma z_2 \equiv 0(modm)$

$\implies \alpha(x_1-x_2)+\beta(y_1-y_2)+\gamma(z_1-z_2) \equiv 0(modm)$

Also,

$|x_1-x_2| \leq [\lambda] \leq \lambda, \qquad |y_1-y_2| \leq [\mu] \leq \mu, \qquad |z_1-z_2| \leq [\nu] \leq \nu$

Let $x=|x_1-x_2|, \qquad y=|y_1-y_2|$ & $\qquad z=|z_1-z_2|$

since the triples are distinct not all of x,y,z can be zero and the result follows.

Lemma 2.3.0.2. *Suppose $ax^2+by^2+c^2$ factored into linear factors modulo m and also modulo n,*

i.e $ax^2+by^2+c^2 \equiv (\alpha x_1+\beta y_1+\gamma z_1)(\alpha x_2+\beta y_2+\gamma z_2)(modm)$

& $ax^2+by^2+c^2 \equiv (\alpha x_3+\beta y_3+\gamma z_3)(\alpha x_4+\beta y_4+\gamma z_4)(modn)$

If $(m,n)=1$, then $ax^2+by^2+c^2$ can be factored into linear factors modulo mn.

Proof:

By the chinese remainder theorem, we my choose $\alpha,\beta,\gamma,\alpha',\beta'\&\gamma'$ to satisfy,

$\alpha \equiv \alpha_1$, $\beta \equiv \beta_1$, $\gamma \equiv \gamma_1$, $\alpha' \equiv \alpha_2$, $\beta' \equiv \beta_2$, $\gamma' \equiv \gamma_2$ $(modm)$

$\alpha \equiv \alpha_3$, $\beta \equiv \beta_3$, $\gamma \equiv \gamma_3$, $\alpha' \equiv \alpha_4$, $\beta' \equiv \beta_4$, $\gamma' \equiv \gamma_4$ $(modn)$

Then the congruence,

$ax^2+by^2+c^2 \equiv (\alpha x+\beta y+\gamma z)(\alpha' x+\beta' y+\gamma' z)$

holds both modulo *m* & modulo *n* and so the congruence holds modulo *mn*.

Theorem 2.3.0.3. *Let $a,b\&c$ be non zero integers such that the product abc is square free, then the equation,*

$$ax^2+by^2+cz^2=0\text{—(1)}$$

is solvable in integers x,y,z not all zero iff

a)The integers a,b,c do not have the same sign.

b)$-bc,-ac$ & $-ac$ are quadratic residues modulo a,b & c

Proof:

If (I) has a solution x_0,y_0 & z_0 not all zero, then it is clear that a,b & c do not have same sign.

If $(x_0,y_0,z_0)=d$ (say)

then divide x_0,y_0 & z_0 by d to obtain x_1,y_1 & z_1 such that $(x_1,y_1,z_1)=1$

T.S.T: $(c,x_1)=1$

suppose $(c,x_1)=p$, for some prime p

$\implies p|c$ & $p|x_1$

since abc is square free, we see that $p\nmid b$ & $p\nmid a$

also, since $p|ax_1^2$, & $p|cz_1^2$

$\implies p|by_1^2$

$\implies p|y_1^2$ {since $p\nmid b$}

$\therefore p^2|ax_1^2+by_1^2$

$\implies p^2|cz_1^2$

Now, since c is square free $\implies p|z_1$

$\therefore (x_1,y_1,z_1)=p$

This is contradiction.

Thus $(c,x_1)=1$

we choose u so that,

$ux_1\equiv 1(modc)$

From (I) we get,

$ax^2+by-1^2\equiv 0(modc)$

$abu^2x^2 + b^2u^2y_1^2 \equiv 0(modc)$ {multiplying bu^2}

$\implies u^2b^2y_1^2 \equiv -ab(modc)$

$\therefore -ab$ is quadratic residue modulo c.

Similarly, $-bc$ & $-ac$ are quadratic residue modulo a & b respt.

Conversely,

Let $-bc, -ac$ & $-ab$ be quadratic residues modulo a, b, c respt.

Note that, if we replace signs of a, b & c then $-bc, -ac$ & $-ab$ are still quadratic residues modulo a, b, c respt.

since a, b & c are all not of same sign, we can always change signs, if necessary so that one is positive and 2 are negative, say $a > 0$ & $b, c < 0$

let r be an integer such that, $r^2 \equiv -ab(modc)$

and a_1 be defined by, $aa_1 \equiv 1(modc)$

This exist since abc is square free $\implies (a,c) = 1$ then,

$$\begin{aligned} ax^2 + by^2 &\equiv aa_1(ax^2 + by^2)(modc) \\ &\equiv a_1(a^2x^2 - r^2y^2)(modc) \\ &\equiv a_1(ax - ry)(ax + ry)(modc) \\ &\equiv (x - a_1ry)(ax + ry)(modc) \end{aligned}$$

Thus $ax^2 + by^2 + cz^2$ is congruent to product of two linear factors modulo c

similarly, $ax^2 + by^2 + cz^2$ is congruent to product of two linear factors modulo a & modulo b.

Thus by lemma 2,, we see that there exist integers $\alpha, \beta, \gamma, \alpha', \beta' \& \gamma'$ such that $ax^2 + by^2 + c^2 \equiv (\alpha x + \beta y + \gamma z)(\alpha' x + \beta' y + \gamma' z)$(mod abc)

since $abc$is square free $\implies (a,b) = (a,c) = (b,c) = 1$

Take $m=abc$,

$\lambda \leq \sqrt{|bc|}, \quad \mu \leq \sqrt{|ac|} \quad \& \ \nu \leq \sqrt{|ab|}$ {by lemma 1}

Then $\exists\, x_1, y_1, z_1 \in \mathbb{Z}$ not all zero such that,

$|x_1| \leq \sqrt{|bc|}, \quad |y_1| \leq \sqrt{|ac|} \quad \& \ |z_1| \leq \sqrt{|ab|}$

and $ax^2+by^2+c^2 \equiv 0 (\text{mod } abc)$

since abc is square free we see that λ is an integer if it is 1 & similarly μ & ν.

Thus we have,

$x_1 \leq bc$ with equality iff $b=c=-1$

$y_1 \leq -ac$ with equality iff $a=1, c=-1$

$z_1 \leq -ab$ with equality iff $a=1, b=-1$

Thus unless $b=c=-1$, we have

$$\begin{aligned} ax^2+by^2+cz^2 &\leq ax_1^2 \\ &< a(bc) = abc \end{aligned}$$

and also we have,

$$\begin{aligned} ax^2+by^2+cz^2 &\geq by^2+c^2 \\ &> b(-ac)+c(-ab) \\ &= -abc \end{aligned}$$

and

$ax^2+by^2+cz^2 \equiv 0 (\text{mod } abc)$

and so we must have either

$ax^2+by^2+c^2=0 \quad$ or $\quad ax^2+by^2+c^2=-abc$

In the first case we have solutions of (I) as x_1, y_1 & z_1.

If the second case obtains,

let $x_2 = -by_1 + x_1z_1, \qquad y_2 = bx_1 + y_1z_1 \qquad \& \; z_2 = z_1^2 + ab$

$$\begin{aligned}\therefore ax_2^2 + by_2^2 + cz_2^2 &= a(-by_1 + x_1z_1)^2 + b(bx_1 + y_1z_1)^2 + c(z_1^2 + ab)^2 \\ &= ab^2y_1^2 + ax_1^2z_1^2 - 2abx_1y_1z_1 + a^2bx_1^2 + by_1^2z_1^2 + 2abx_1y_1z_1 + cz_1^4 \\ &+ a^2b^2c + 2abcz_1^2 \\ &= z_1^2(ax_1^2 + by_1^2 + cz_1^2) + ab(ax_1^2 + by_1^2 + cz_1^2) + abcz_1^2 + a^2b^2c \\ &= z_1^2(-abc) + ab(-abc) + abcz_1^2 + a^2b^2c \\ &= 0\end{aligned}$$

$\therefore x_2, y_2, z_2$ is a solution of (1).

In case of $x_2 = y_2 = z_2 = 1$ then,

$z_1^2 + ab = 0$

$\implies z_1^2 = -ab$

$\therefore z_1 = \pm 1 \qquad \{\because ab$ are square free then $a = 1$ & $b = -1\}$

and $x_3 = 1, \qquad y_3 = -1, \qquad z_3 = 0$ is a solution of (1).

Finally,

Suppose $b = c = -1$, then -1 is quadratic residue modulo a.

There's a result that says,

Let R(n) denote the number of roots of $S^2 \equiv -1$***(mod*** n***) then P(n)=R(n) for*** $n >$ 1***,P(1)=2, R(1)=1, Q(1)=4, Q(n)=4R(n) for*** $n \geq 1$ ***&*** $N(n) = 4\sum_{d^2|n} R(n|d^2)$

N(n)- Number of solutions of $x^2 + y^2 = n$***.***

P(n)- Number of non-negative primitive solutions of $x^2 + y^2 = n$***.***

Q(n)- Number of primitive solutions of $x^2 + y^2 = n$.

This implies that Q(a) is positive & hence that the equation $y^2 + z^2 = a$ has a solution y_1, z_1.

Then $x = 1, \quad y = y_1, \quad z = z_1$ is a solution of (1) since $b = c = -1$.

Chapter 3

LINEAR DIOPHANTINE EQUATIONS

The data for this chapter is collected from [5].
We know that Diophantine equation is a polynomial equation with 2 or more integer unknowns. A linear Diophantine equation with 2 or more integer unknowns and the integer unknowns are each to at most of degree 1.

In this chapter we will learn about linear Diophantine equation and how to find it's solutions.

3.1 The Equation $ax + by = c$

Any linear equation in two variables having integral coefficient can be put in the form,

. $$ax + by = c$$

This problem is trivial unless neither a nor b is zero.

Theorem 3.1.0.1. *If $d = (a,b)$ is g.c.d of a & b, then $\exists\, x_0, y_0 \in \mathbb{Z}$ such that $d = ax_0 + by_0$.*

Proof:

Consider a linear combination $ax+by$, where x & y range over all integers.

let S=$\{c \in \mathbb{Z} / \ c = ax+by \ ; a,b,x,y \in \mathbb{Z}\}$

choose $x_0, y_0 \in \mathbb{Z}$ such that $ax_0 + by_0 = d$ is least in S.

T.S.T:$d|a$ & $d|b$.

Using division algorithm for a & b $\exists$ $q, r \in \mathbb{Z}$ such that $a = qd + r$

where $0 \leq r \leq d$

If suppose $r \neq 0$

$\implies a = qd + r$

$\implies r = a - qd$

$\implies r = a - q(ax_0 + by_0))$

$\implies r = a(1 - qx_0) + b(qy_0)$

$\implies r \in S$

This is contradiction since d is the least element in S.

$\therefore r = 0$

$\implies a = qd$

i.e $d|a$

similarly, $d|b$

$\therefore d$ is common divisor of a & b.

T.S.T: d is the g.c.d of a & b.

let c be a common divisor of a & b.

i.e $c|a$ & $c|b$

$\implies c|ax+by \qquad ; x,y \in \mathbb{Z}$

In particular,

$c|ax_0+by_0$

$\implies c|d$

since c was an arbitrary common divisor of a & b. we have $d=(a,b)$.

NOTE:

1. The linear diophantine equation $ax+by=c$ has a solution iff $d|c$, where $d=(a,b)$

   Proof:

   Let $d=(a,b)$

   $\implies d|a$ & $d|b$

   $a=dr \qquad \& \qquad b=ds \qquad ; s,r \in \mathbb{Z}.$

   suppose $ax+by=c$ has a solution, then $\exists x_1,y_1 \in \mathbb{Z}$, such that,

   $$\begin{aligned} c &= ax_1+by_1 \\ &= drx_1+dsy_1 \\ &= d(rx_1+sy_1) \end{aligned}$$

   $\implies d|c$

   conversely,

   Let $d|c \implies c=dt \qquad t \in \mathbb{Z}$

   & let $d=gcd(a,b)$

   $\implies d=ax_0+by_0$ for some $x_0,y_0 \in \mathbb{Z}$

   $$\begin{aligned} \because c &= dt \\ &= (ax_0+by_0)t \\ &= a(x_0t)+b(y_0t) \end{aligned}$$

$\therefore x_0t + y_0t$ is a particular solution to $ax + by = c$.

2. If $x_0, y_0 \in \mathbb{Z}$is any particular solution of $ax + by = c$, then all other solutions are given by,

   $x = x_0 - (\frac{b}{d})t \quad ,y = y_0 - (\frac{a}{d})t \quad ; t \in \mathbb{Z}$

   Proof:

   Let x_0 & y_0 be a particular solution to $ax + by = c$ i.e $ax_0 + by_0 = c$

   Let x', y' be another solution of $ax + by = c$, i.e $ax' + by' = c$

   $\therefore ax' + by' = ax_0 + by_0 = c$

   i.e $a(x_0 - x') = b(y' - y_0)$ ——-(a)

   If d=(a,b)

   i.e $d|a$ & $d|b$

   $\implies a = dr$ & $b = ds \quad ;r, s \in \mathbb{Z}$ & $(r, s) = 1$

   $\therefore$ (a) $\implies dr(x_0 - x') = ds(y' - y_0)$

   $\implies r(x_0 - x') = s(y' - y_0)$

   i.e $r|s(y' - y_0)$

   $\implies r|(y' - y_0) \quad \because (r, s) = 1$

   $\implies y' - y_0 = rt$

   $\implies y' = y_0 + (\frac{a}{d})t$

   similarly,

   $x' = x_0 - st$

   $\implies x' = x_0 - (\frac{b}{d})t$

3.2 The Equation $a_1x_1 + a_2x_2 + \cdots + a_kx_k = c$

Theorem 3.2.0.1. *The equation $a_1x_1 + a_2x_2 + \cdots + a_kx_k = c$ ——(1) ;$k \geq 2$, has a solution iff $d|c$, where $d = gcd(a_1, a_2, \ldots, a_k)$.*

Proof:

If (1) has a solution then $d|c$.

conversely,

Suppose $d|c$, where $d = gcd(a_1, a_2, \ldots, a_k)$.

$\because d = gcd(a_1, a_2, \ldots, a_k)$

$\implies \exists$ integers $y_1, y_2, \ldots, y_k$ such that,

$a_1y_1 + a_2y_2 + \cdots + a_ky_k = d$

$\implies r(a_1y_1 + a_2y_2 + \cdots + a_ky_k) = dr$

$\implies r(a_1y_1 + a_2y_2 + \cdots + a_ky_k) = c \qquad \{\because d|c \implies c = dr, r \in \mathbb{Z}\}$

$\therefore x_1 = ry_1, x_2 = ry_2, \ldots, x_k = ry_k$ is a solution of (1).

To find solution of (1) we reduce it to the case with 2 unknowns:

Suppose that $a_i \neq 0$,$1 \leq i \leq k$ & $d|c$; $d = gcd(a_1, a_2, \ldots, a_k)$

Let $x_{k-1} = \alpha u + \beta v$——(i)

& $x_k = \gamma u + \delta v$——(ii)

where $\alpha, \beta, \gamma, \delta \in \mathbb{Z}$ such that $\alpha\delta - \beta\gamma = 1$

$$\begin{aligned} \therefore \delta x_{k-1} - \beta x_k &= \alpha\delta u + \beta\delta v - \gamma\beta u + \beta\delta v \\ &= u(\alpha\delta - \beta\gamma) \\ &= u \end{aligned}$$

$\Longrightarrow u = \delta x_{k-1} - \beta x_k$

Similarly,

$v = -\gamma x_{k-1} + \alpha x_k$

Thus $u, v \in \mathbb{Z}$ iff $x_{k-1}, x_k \in \mathbb{Z}$

If we take,

$\beta = \frac{a_k}{(a_{k-1}, a_k)}$ & $\delta = \frac{a_{k-1}}{(a_{k-1}, a_k)}$

Then (β, δ), and we solve $\alpha\delta - \beta\gamma = 1$ to find α, γ by the method used for unknowns.

Consider,

$$\begin{aligned} a_{k-1}x_{k-1} + a_k x_K &= a_{k-1}(\alpha u + \beta v) + a_k(\gamma u + \delta v) \\ &= (a_{k-1}\alpha + a_k\gamma)u + (a_{k-1}\beta + a_k\delta)v \\ &= (a_{k-1}\alpha + a_k\gamma)u + \left[\frac{a_{k-1}a_k}{(a_{k-1}, a_k)} - \frac{a_{k-1}a_k}{(a_{k-1}, a_k)}\right] v \\ &= (a_{k-1}\alpha + a_k\gamma)u \end{aligned}$$

Equation (1) now reduces to,

$a_1x_1 + a_2x_2 + \cdots + a_{k-2}x_{k-2} + (a_{k-1}\alpha + a_k\gamma)u = c$ ——-(A)

Note that,

$$\begin{aligned} a_{k-1}\alpha + a_k\gamma &= -(a_{k-1}, a_k)\alpha\delta + (a_{k-1}, a_k)\beta\gamma \\ &= -(a_{k-1}, a_k)[\alpha\delta - \beta\gamma] \\ &= -(a_{k-1}, a_k) \end{aligned}$$

Thus $(a_1, a_2, \ldots, a_{k-2}, (a_{k-1}, a_k)) = (a_1, a_2, \ldots, a_k)$

$\therefore$. The new equation (A) has the same property as (1) that the gcd of it's coefficients divides c & that no coefficient is zero.

If $k > 3$, this reduction process can be applied to equation (A) to produce an equation with $k-2$ variables & hence repetition of the of the process finally lead to an equation with two unknowns, and hence the result.

EXERCISE:

Q1: Solve the following:

(a) $172x + 20y = 1000$

Soln:

Using Euclidean algorithm on $a = 172$ & $b = 20$

$$\begin{aligned}\therefore 172 &= 8(20) + 12\\ 20 &= 1(12) + 8\\ 12 &= 1(8) + 4\\ 8 &= 2(4) + 0\end{aligned}$$

$\therefore gcd(172,20) = 4 \quad \& \quad 4|1000$

$$\begin{aligned}4 &= 12 - 1(8)\\ &= 12 - (20 - 1(12))\\ &= -20 + 2(12)\\ &= -20 + 2(172 - 8(20))\\ &= 2(172) - 17(20)\end{aligned}$$

$\therefore 4 = 2(172) - 17(20) \implies 1000 = 500(172) - 4250(20)$ {multiply 250 throught}

Thus $(x_0, y_0) = (500, -4250)$ is one of the solutions.

$$\therefore x = x_0 + \frac{b}{d}t = 500 + \frac{20}{4}t = 500 + 5t$$

$$\&y = y_0 + \frac{a}{d}t = -4250 + \frac{172}{4}t = -4250 - 43t$$

Thus $(x, y) = (500 + 5t, -4250 - 43t)$ are solutions.

(b) $6x + 51y = 20$

Soln:

For $a = 6$ & $b = 51$

$$51 = 7(6) + 3$$

$$6 = 2(3) + 0$$

$\therefore gcd(6, 51) = 3 \quad \& \quad 3 \nmid 20$

$\therefore 6x + 51y = 20$ does not have a solution.

Q2: Find the solution of the equation $8x + 6y + 14z = 10$, if it exists.

Soln:

Here $gcd(8, 6, 14) = 2$ and $2|10$, hence the solution exists.

Firstly,

$$let \;\; 6y + 14z = gcd(6, 14)u = 2u \quad where \;\; u \in \mathbb{Z}$$

$\therefore 8x + 2u = 10$ which is a linear Diophantine equation with 2 variables.

Here, $8(1) + 2(1) = 10$

Thus $(x_0, u_0) = (1, 1)$ is one of the solution of $8x + 2u = 10$.

$$\therefore x = 1 + \frac{1}{1}t = 1 + t \quad \& \quad u = 1 - \frac{4}{1}t = 1 - 4t, \quad t = 0, \pm 1, \pm 2, \ldots$$

are other solutions of $8x + 2u = 10$.

consider,

$6y + 14z = 2$,

We see that $(y_0, z_0) = (-2, 1)$ satisfies the above equation.

Thus $(y_0, z_0) = (-2u, u)$ satisfies $6y + 14z = 2u$

$$\therefore y = -2u + \frac{7}{1}s = -2 + 4t + 7s \quad \& \quad z = u - \frac{3}{1}s = 1 - 4t - 3s, \quad s = 0, \pm 1, \pm 2, \ldots$$

Thus $(x, y, z) = (1 + t, -2 + 8t + 7s, 1 - 4t - 3s)$ is the set solutions.

Chapter 4

PELL'S EQUATIONS

Data in this part are taken from [2].
Let d be a positive integer which is not a perfect square, the equation

$$x^2 - dy^2 = 1$$

is called pell's equation.

The requirement that d is not the square of a whole number is equivalent to the fact that the number $\sqrt{d}$ is irrational.

Once a solution in integers to pell's equation is given it is possible to generate infinitely many others.Underlying this is an algebraic structure that can be revealed through operation on quadratic surds.

4.1 Quadratic Surds

Let a, b, d be rational numbers with d as non square positive integer. A quadratic surd is a number of the form $a+b\sqrt{d}$.

It's surd conjugate is given by,

$$\overline{a+b\sqrt{d}} = a-b\sqrt{d}$$

Multiplying a quadratic surd by it's conjugate gives it's norm and is denoted by,

$$N(a+b\sqrt{d}) = a^2 - b^2 d$$

$\therefore$The norm of surd has the same form as the left side of Pell's equation, it is not surprising that surds have a role to play in the analysis of the equation.

EXERCISE:

Q1: Write the product of $2+7\sqrt{3}$ & $3-4\sqrt{3}$ in the form $a+b\sqrt{d}$, where a & b are integers.

Soln:

$$\begin{aligned}(2+7\sqrt{3})(3-4\sqrt{3}) &= (2\times 3 - 7\times 4\times 3) - (2\times 4 + 3\times 7)\sqrt{3} \\ &= -78 + 13\sqrt{3}\end{aligned}$$

Q2: What are the norms of $2+7\sqrt{3}$ & $3-4\sqrt{3}$.

Soln:

$$\begin{aligned}N(2+7\sqrt{3}) &= 2^2 - 7^2\times 3 \\ &= -143\end{aligned}$$

$$\begin{aligned}N(3-4\sqrt{3}) &= 3^2 - 4^2\times 3 \\ &= -39\end{aligned}$$

Q3: Write $(2+7\sqrt{3})^{-1}$ in the form $u+v\sqrt{3}$, where $u,v \in \mathbb{Q}$.

Soln:

$$\begin{aligned}(2+7\sqrt{3})^{-1} &= \frac{1}{2+7\sqrt{3}} \times \frac{2-7\sqrt{3}}{2-7\sqrt{3}} \\ &= \frac{2-7\sqrt{3}}{4-49\times 3} \\ &= \frac{-2}{143} + \frac{7}{143}\sqrt{3}\end{aligned}$$

Q4: Observe that $2+\sqrt{3}$ has a multiplicative inverse $p+q\sqrt{3}$, where p & q are not merely rationals but integers.

Soln:

$(2+\sqrt{3})(p+q\sqrt{3}) = 1$

$\implies 2p+3q+2q\sqrt{3}+p\sqrt{3} = 1$

$\implies (2p+3q)+(2q+p)\sqrt{3} = 1$

$\implies 2p+3q = 1 \quad \& \quad 2q+p = 0$

solving these equations simultaneously we get,

$p = 2$ & $q = -1$

$\therefore 2-\sqrt{3}$ is multiplicative inverse of $2+\sqrt{3}$.

RESULTS:

For $c = a+b\sqrt{d} \quad \& \quad w = u+v\sqrt{d}$, then

(i) $\overline{cw} = \overline{c} \times \overline{w}$

(ii) $N(cw) = N(c)N(w)$

(iii) $N(c+w)+N(c-w) = 2[N(c)+N(w)]$

(iv) $\frac{c}{w} = \frac{c\overline{w}}{N(w)}$

Proof:

$$\begin{aligned} cw &= (c = a + b\sqrt{d})(w = u + v\sqrt{d}) \\ &= (au + bdv) + (av + bu)\sqrt{d} \end{aligned}$$

$$\begin{aligned} (i) \therefore \overline{cw} &= (au + bdv) - (av + bu)\sqrt{d} \\ &= a(u + v\sqrt{d}) - b\sqrt{d}(u + v\sqrt{d}) \\ &= (u + v\sqrt{d})(a + b\sqrt{d}) \\ &= \overline{c} \times \overline{w} \end{aligned}$$

$$\begin{aligned} (ii) N(cw) &= (au + bdv)^2 + (av + bu)^2 d \\ &= (au)^2 + (bdv)^2 + 2aubdv - (av)^2 d - (bu)^2 d - 2abduv \\ &= a^2(u^2 - v^2 d) - b^2 d(u^2 - v^2 d) \\ &= (a^2 - b^2 d)(u^2 - v^2 d) \\ &= N(c)N(w) \end{aligned}$$

$$\begin{aligned} (iii) \quad & c + w = (a + u) + (b + v)\sqrt{d} \\ & \& \ c - w = (a - u) + (b - v)\sqrt{d} \end{aligned}$$

$$\begin{aligned} \therefore N(c + w) + N(c - w) &= (a + u)^2 + (b + v)^2 d + (a - u)^2 + (b - v)^2 d \\ &= a^2 + u^2 + 2au - [b^2 + v^2 + 2bv]d + a^2 + u^2 - 2au - \\ &\quad [b^2 + v^2 - 2bv]d \\ &= 2a^2 + 2u^2 - [2b^2 + 2v^2]d \\ &= 2[a^2 - b^2 + u^2 - v^2] \\ &= 2[N(c) + N(w)] \end{aligned}$$

$$\begin{aligned} (iv) \tfrac{c}{w} &= \tfrac{c}{w} \times \tfrac{\overline{w}}{\overline{w}} \\ &= \tfrac{c\overline{w}}{N(w)} \end{aligned}$$

NOTE:

Pell's equation can be written in the form,

$$N(x+y\sqrt{d}) = k$$

EXERCISE:

Q1: Suppose that $x^2 - dy^2 = k$ & $u^2 - dv^2 = l$ are two given integer equation. Define the integers m & n by,

$$m+n\sqrt{d} = (x+y\sqrt{d})(u+v\sqrt{d})$$

verify that $m = xu+dyv$, $n = xv+yu$ & $m^2 - dn^2 = kl$

Soln:

We are given that,

$$\begin{aligned} m+n\sqrt{d} &= (x+y\sqrt{d})(u+v\sqrt{d}) \\ &= (xu+yvd)+(xv+yu)\sqrt{d} \end{aligned}$$

$\therefore$ we get,

$m = xu+dyv$ & $n = xv+yu$

Also,

$$\begin{aligned} (m+n\sqrt{d})(m-n\sqrt{d}) &= [(xu+dyv)+(xv+yu)\sqrt{d}] \\ &\quad \times[(xu+dyv)-(xv+yu)\sqrt{d}] \end{aligned}$$

$$\begin{aligned} \therefore m^2 - n^2 d &= (xu+dyv)^2 - (xv+yu)^2 d \\ &= x^2u^2 + y^2v^2d^2 + 2xyvud - x^2v^2d - y^2u^2d - 2xyuvd \\ &= x^2(u^2 - v^2d) - y^2d(u^2 - v^2d) \\ &= (x^2 - y^2d)(u^2 - v^2d) \\ &= kl \end{aligned}$$

Q2: (a) Suppose that $(x,y) = (x_1,y_1)$ is solution to $x^2 - dy^2 = 1$. Define the integer pair (x_2,y_2) by equation

$$x_2 + y_2\sqrt{d} = (x_1 + y_1\sqrt{d})^2$$

Verify that $x_2 = x_1^2 + dy_1^2, \quad y_2 = 2x_1y_1 \quad \& \quad (x_2,y_2)$ is a solution of $x^2 - dy^2 = 1$.

(b) More generally suppose that (x_n,y_n) is defined by

$$x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n, \quad for\ n \geq 2$$

Note that, $x_n + y_n\sqrt{d} = (x_{n-1} + y_{n-1}\sqrt{d})(x_1 + y_1\sqrt{d})$

& deduce that $x_n = x_1x_{n-1} + dy_1y_{n-1} \quad \& \quad y_n = x_1y_{n-1} + y_1x_{n-1}$

Prove that (x_n,y_n) is a solution of $x^2 - dy^2 = 1$.

Soln:

(a) Given that,

$$\begin{aligned} x_2 + y_2\sqrt{d} &= (x_1 + y_1\sqrt{d}^2) \\ &= (x_1^2 + y_1^2 d) + 2x_1y_1\sqrt{d} \end{aligned}$$

$\therefore x_2 = x_1^2 + dy_1^2, \quad y_2 = 2x_1y_1$

To check if (x_2,y_2) is a solution of $x^2 - dy^2 = 1$.

$$\begin{aligned} x_2^2 - dy_2^2 &= (x_1^2 + dy_1^2)^2 - (2x_1y_1)^2 \\ &= (x_1^2)^2 + (y_1^2 d)^2 - 2x_1^2y_1^2 d \\ &= (x_1^2 - dy_1^2)^2 \\ &= (1)^2 \qquad\qquad \{\because (x_1,y_1)\ is\ a\ solution\} \\ &= 1 \end{aligned}$$

$\therefore (x_2,y_2)$ is a solution of $x^2 - dy^2 = 1$.

(b) We use induction on n,

For $n = 2$ the result holds $\quad$ {from (a)}

i.e $x_2+y_2\sqrt{d}=(x_1+y_1\sqrt{d})^2$ & (x_2,y_2) is a solution of $x^2-dy^2=1$

Assume that result holds for $n=k>2$

i.e $x_k+y_k\sqrt{d}=(x_1+y_1\sqrt{d})^k$ & (x_k,y_k) is a solution of $x^2-dy^2=1$

Consider for $n=k+1$

$$\begin{aligned} x_{k+1}+y_{k+1}\sqrt{d} &= (x_k+y_k\sqrt{d})(x_1+y_1\sqrt{d}) \\ &= (x_1+y_1\sqrt{d})^k(x_1+y_1\sqrt{d}) \qquad \{by \quad induction \quad hypothesis\} \\ &= (x_1+y_1\sqrt{d})^{k+1} \\ &= 1 \end{aligned}$$

$\therefore (x_n,y_n)$ is a solution of $x^2-dy^2=1$.

Also from $x_{k+1}+y_{k+1}\sqrt{d}=(x_k+y_k\sqrt{d})(x_1+y_1\sqrt{d})$ we get,

$x_{k+1}=x_1x_k+dy_1y_k$ & $y_{k+1}=x_1y_k+y_1x_k$

Hence by induction hypothesis the result holds.

Q3: Show that there are an infinite number of solution in integers of the simultaneous equation,

$$\begin{aligned} x^2-1&=(u+1)(v-1) \\ y^2-1&=(u-1)(v+1) \end{aligned} \quad \text{———(A)}$$

(a) Suppose that the two equation are satisfied. Deduce that,

$$(v+1)x^2-(v-1)y^2=2v^2$$

Soln:

From (A) we get,

$$\frac{x^2-1}{v-1}=u+1 \quad \& \quad \frac{y^2-1}{v+1}=u-1$$

Subtracting both we get,

$\frac{x^2-1}{v-1} - \frac{y^2-1}{v+1} = 2$

$\implies (x^2-1)(v+1) - (y^2-1)(v-1) = 2(v^2-1)$

$\implies (v+1)x^2 - v - 1 - (v-1)y^2 + v - 1 = 2v^2 - 2$

$\implies (v+1)x^2 - (v-1)y^2 = 2v^2$

(b) Making the substitution $v = 2w, \quad r = \frac{x}{v} \quad \& \; s = \frac{y}{v}$ obtain from **(a)** that,

$$(w+\frac{1}{2})r^2 - (w-\frac{1}{2})r^2 = 1$$

Soln:

Given that,

$(v+1)x^2 - (v-1)y^2 = 2v^2 \qquad \{from \quad (a)\}$

$\implies (\frac{1}{v} + \frac{1}{v^2})x^2 - (\frac{1}{v} - \frac{1}{v^2})y^2 = 2$

$\implies (v+1)r^2 - (v-1)r^2 = 2 \qquad \{substitute \quad x = rv \quad \& \quad y = sv\}$

$\implies (2w+1)r^2 - (2w-1)s^2 = 2 \qquad \{substitute \quad v = 2w\}$

$\implies (w+\frac{1}{2})r^2 - (w-\frac{1}{2})s^2 = 1$

(c) Let w be arbitrary, Determine a simple numerical solution of the equation in **(b)**.

Soln:

Given that,

$(w+\frac{1}{2})r^2 - (w-\frac{1}{2})s^2 = 1 \quad$ & w is arbitrary.

$\implies (w+\frac{1}{2})r^2 = 1 + (w-\frac{1}{2})s^2$

$\implies (w-\frac{1}{2})r^2 + r^2 = 1 + (w-\frac{1}{2})s^2$

Comparing both sides we get,

$r^2 = s^2 \quad \& \quad r^2 = 1$

$\implies r = s \quad \& \quad r = \pm 1$

Hence $r = s = \pm 1$ & simplest solution is given by $(r,s) = (\pm r, \pm s)$

(d) Explain how **(c)** lead to the result that if $(r,s) = (r_0, s_0)$ satisfy the equation in **(b)**, then so also does $(r,s) = (r_n, s_n)$ defined recursively by,

$$r_{n+1} = 2wr_n + (2w-1)s_n$$

$$\& s_{n+1} = (2w+1)r_n + 2ws_n$$

Soln:

We will use induction on n,

for $n = 0$,

$r_1 = 2wr_0 + (2w-1)s_0 \qquad \& \qquad s_1 = (2w+1)r_0 + 2ws_0$

$\therefore$ equation in (b) becomes,

$$\begin{aligned}
(w+\frac{1}{2})r_1^2 - (w-\frac{1}{2})s_1^2 &= (w+\frac{1}{2})[2wr_0 + (2w-1)s_0]^2 - (w-\frac{1}{2})[(2w+1)r_0 + 2ws_0]^2 \\
&= (w+\frac{1}{2})[4w^2r_0^2 + (2w-1)^2s_0^2 + 4w(2w-1)r_0s_0] \\
&\quad - (w-\frac{1}{2})[(2w+1)^2r_0^2 + 4w^2s_0^2 + 4w(2w+1)r_0s_0] \\
&= 4w^2[(w+\frac{1}{2})r_0^2 - (w-\frac{1}{2})s_0^2] \\
&\quad + 4wr_0s_0[(w+\frac{1}{2})(2w-1) - (w-\frac{1}{2})(2w+1)] \\
&\quad + (w+\frac{1}{2})(2w-\frac{1}{2})^2s_0^2 - (w-\frac{1}{2})(2w+1)^2r_0^2 \\
&= 4w^2(1) + 4wr_0s_0[2\{[(w+\frac{1}{2})(w-\frac{1}{2}) - (w-\frac{1}{2})(w+\frac{1}{2})\}] \\
&\quad + (w+\frac{1}{2})(2w-1)^2s_0^2 - (w-\frac{1}{2})(2w+1)^2r_0^2
\end{aligned}$$

$$\begin{aligned}\textbf{i.e}(w+\frac{1}{2})r_1^2-(w-\frac{1}{2})s_1^2 &= 4w^2+4s_0^2(w+\frac{1}{2})(w-\frac{1}{2})^2-4(w+\frac{1}{2})^2(w-\frac{1}{2})r_0^2\\ &= 4w^2+4[s_0^2(w^2-\frac{1}{4})(w-\frac{1}{2})-r_0^2(w+\frac{1}{2})(w^2-\frac{1}{4})]\\ &= 4w^2-4(w^2-\frac{1}{4})[r_0^2(w+\frac{1}{2})-s_0^2(w-\frac{1}{2})]\\ &= 4w^2-4w^2+1\\ &= 1\end{aligned}$$

$\therefore$ result holds for $n=0$

Assume that result holds for $n=k$.

i.e $r_k = 2wr_{k-1}+(2w-1)s_{k-1}$

& $s_k = (2w+1)r_{k-1}+2ws_{k-1}$

& $(w+\frac{1}{2})r_k^2-(w-\frac{1}{2})s_k^2 = 1$

Consider for $n=k+1$,

$r_{k+1} = 2wr_k+(2w-1)s_k$

& $s_{k+1} = (2w+1)r_k+2ws_k$

Following the same pattern as in base case we see that,

$(w+\frac{1}{2})r_{k+1}^2-(w-\frac{1}{2})s_{k+1}^2 = 1$

$\therefore$ By induction the result holds.

4.2 Existence of rational solution

It is natural to ask whether $x^2-dy^2=1$ has a solution other than the trivial $(x,y)=(\pm1,0)$, where d is positive non square integer. An investigation suggested an affirmative

answer,although for some values of d, the solutions are very difficult to find.

Here are some of smallest solutions for low values of d.

d	**(x,y)**
2	(3,2),(17,12)
3	(2,1),(7,4)
5	(9,4),(161,72)
6	(5,2),(49,20)
7	(8,3),(127,48)
8	(3,1),(17,6)

d	**(x,y)**
10	(19,6)
11	(10,3)
12	(7,2),(97,28)
13	(649,180)
14	(15,4)
15	(4,1)(31,8)

One way to approach the problem is to ask for solution that are rational, and use these to get integer solution.

EXERCISE:

Q1: Determine the solution of the equation, where c is any integer such that $(x,y) = (c,1)$

$$x^2 - dy^2 = (c^2 - d)^2$$

Soln:

Given that,

$$\begin{aligned} x^2 - dy^2 &= (c^2 - d)^2 \\ &= c^4 + d^2 - 2c^2 d \\ &= c^4 + 2c^2 d + d^2 - 2c^2 d - 2c^2 d \\ &= (c^2 + d) - (2c)^2 d \end{aligned}$$

$\implies x = c^2 + d \quad \& \quad y = 2c$

Thus $(x,y) = (c^2 + d, 2c)$ is a solution.

Q2: Describe how to determine solutions of $x^2 - dy^2 = 1$ for which x & y are rational, but not necessarily integers.

Soln:

Given equation can be written as,

$$\begin{aligned} x^2 - dy^2 &= \frac{(c^2-d)^2}{(c^2-d)^2} \\ &= \frac{(c^2+d)^2}{(c^2-d)^2} - \frac{(2c)^2}{(c^2-d)^2} \qquad \{solve \ \ as \ \ in \ \ \mathbf{Q1}\} \\ \implies x = \frac{c^2+d}{c^2-d} \ \ &\& \ \ y = \frac{2c}{c^2-d} \end{aligned}$$

Thus $(x,y) = (\frac{c^2+d}{c^2-d}, \frac{2c}{c^2-d})$ is a solution.
{where $c \in \mathbb{Z}$ such that $(x,y) = (c,1)$ is a solution of $x^2 - dy^2 = (c^2-d)^2$}.

Q3: Solve in positive integers the equation $x^2 - 13y^2 = 3^2$ & derive a rational solution of $x^2 - 13y^2 = 1$.

Soln:

We know that solution for $x^2 - dy^2 = (c^2-d)^2$ in integers is given by $(x,y) = (c^2+d, 2c)$ & in rationals is given by $(x,y) = (\frac{c^2+d}{c^2-d}, \frac{2c}{c^2-d})$.

In this case,
$d = 13 \ \ \& \ \ c^2 - d = 3 \implies c = \sqrt{3+13} = 4$

$\therefore$ Solution in integers is $(x,y) = (c^2+d, 2c) = (29,8)$ & in rationals is $(x,y) = (\frac{c^2+d}{c^2-d}, \frac{2c}{c^2-d}) = (\frac{29}{3}, \frac{8}{3})$.

Q4: Find the smallest solution in positive integers of $x^2 - 13y^2 = 2^2$.

Soln:

Consider,
$x^2 - 13y^2 = 2^2$

$\implies 13y^2 = x^2 - 2^2$

$\implies 13y^2 = (x-2)(x+2)$

$\therefore$ either $x-2 = 13k$ or $x+2 = 13k$

Thus we try for $x = 2, 11, 15, 24, 28, \ldots$

$\therefore$we have (11-2)(11+2)=13×3^2

Hence $(x,y) = (11,3)$ is a solution.

4.3 Power Of Solution

Suppose d is a non square integer & that $(x,y) = (u,v)$ is a solution of $x^2 - dy^2 = 1$. For a positive integer n, let (x_n, y_n) be determined by

$$x_n + y_n\sqrt{d} = (u + v\sqrt{d})^n$$

The numbers x_n & y_n can be determined recursively by,

$$x_{n+1} = ux_n + dvy_n$$

$$y_{n+1} = vx_n + uy_n$$

However, it is possible to derive expression for x_n & y_n as polynomials in u & v.

EXERCISE:

Q1: Using the fact that $dv^2 = u^2 - 1$,

(a)verify that,

$(x_1, y_1) = (u, v)$

$(x_2, y_2) = (2u^2 - 1, 2uv)$

$(x_3, y_3) = (4u^3 - 3u, (4u^2 - 1)v)$

are solutions of $x_n + y_n\sqrt{d} = (u + v\sqrt{d})^n$.

Soln:

For $n = 1$

$x_1 + y_1\sqrt{d} = u + v\sqrt{d}$

$\therefore (x_1, y_1) = (u, v)$

For $n = 2$

$$\begin{aligned} x_2 + y_2\sqrt{d} &= (u + v\sqrt{d})^2 \\ &= u^2 + v^2 d + 2uv\sqrt{d} \\ &= u^2 + (u^2 - 1) + 2uv\sqrt{d} \\ &= 2u^2 - 1 + 2uv\sqrt{d} \end{aligned}$$

$\therefore (x_2, y_2) = (2u^2 - 1, 2uv)$

For $n = 3$

$$\begin{aligned} x_3 + y_3\sqrt{d} &= (u + v\sqrt{d})^3 \\ &= u^3 + 3u^2 v\sqrt{d} + 3uv^2 d + v^3 d\sqrt{d} \\ &= u^3 + 3u(u^2 - 1) + (3u^2 + u^2 - 1)v\sqrt{d} \\ &= 4u^3 - 3u + (4u^2 - 1)v\sqrt{d} \end{aligned}$$

$\therefore (x_3, y_3) = (4u^{3-3u}, (4u^2 - 1)v)$

(b) Observe that,

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} u & dv \\ v & u \end{pmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix}$$

Verify that, $\begin{pmatrix} u & dv \\ v & u \end{pmatrix}^2 = 2u \begin{pmatrix} u & dv \\ v & u \end{pmatrix} - \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

& also deduce that,

$$x_{n+1} = 2ux_n - x_{n-1}y_{n+1} = 2uy_n - y_{n-1}$$

for $n \geq 1$, where $(x_0, y_0) = (1,0)$ & $(x_1, y_1) = (u, v)$

Soln:

$$\begin{pmatrix} u & dv \\ v & u \end{pmatrix}^2 = \begin{pmatrix} u^2 + v^2 d & uvd + uvd \\ uv + uv & v^2 d + u^2 \end{pmatrix}$$

$$= \begin{pmatrix} u^2 + u^2 - 1 & 2uvd \\ 2uv & u^2 - 1 + u^2 \end{pmatrix}$$

$$= 2u \begin{pmatrix} u & dv \\ v & u \end{pmatrix} - \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Also,

$$\begin{aligned} \begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} &= \begin{pmatrix} u & dv \\ v & u \end{pmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix} \\ &= \begin{pmatrix} u & dv \\ v & u \end{pmatrix} \begin{pmatrix} u & dv \\ v & u \end{pmatrix} \begin{pmatrix} x_{n-1} \\ y_{n-1} \end{pmatrix} \\ &= \left[2u \begin{pmatrix} u & dv \\ v & u \end{pmatrix} - \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right] \begin{pmatrix} x_{n-1} \\ y_{n-1} \end{pmatrix} \\ &= 2u \begin{pmatrix} u & dv \\ v & u \end{pmatrix} \begin{pmatrix} x_{n-1} \\ y_{n-1} \end{pmatrix} - \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x_{n-1} \\ y_{n-1} \end{pmatrix} \end{aligned}$$

$$\implies \begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = 2u \begin{pmatrix} x_n \\ y_n \end{pmatrix} - \begin{pmatrix} x_{n-1} \\ y_{n-1} \end{pmatrix}$$

$$\implies \begin{pmatrix} x_{n-1} \\ y_{n-1} \end{pmatrix} = \begin{pmatrix} 2ux_n - x_{n-1} \\ 2uy_n - y_{n-1} \end{pmatrix}$$

Hence $x_{n+1} = 2ux_n - x_{n-1}$ & $y_{n+1} = 2uy_n - y_{n-1}$

4.4 Chebyshev Polynomial

Chebyshev polynomial turn up in variety of mathematical contexts and have a number of remarkable properties. We look at a few of them in this section & will define them as new and show that our definition is consistant with that of previous section.

For $-1 < t < 1$, determine θ such that $0 < \theta < \pi$ & $t = \cos\theta$
$\{\therefore \theta = \arccos t\}$

Define,

$$T_n(t) = \cos n\theta = \cos(n \arccos t)$$

&

$$U_n(t) = \frac{\sin n\theta}{\sin\theta} = (1-t^2)^{-\frac{1}{2}} \sin(n \arccos t)$$

Here T_n are called Chebyshev polynomial of the first kind & U_n are called Chebyshev polynomial of second kind.

While these functions are initially defined on restricted domain, they turn out to be

polynomials in t & so have meaning for all real values of t.

EXERCISE:

Q1: Consider the equation $x^2-(t^2-1)y^2=1$, where t is a parameter. An obvious solution is $(x,y)=(t,1)$. Other solutions can be obtained from

$$x_n+\sqrt{t^2-1}y_n=(t+\sqrt{t^2-1})^n=(t+i\sqrt{1-t^2})^n$$

Writting $t=\cos\theta$ & using Moivre's theorem, verify that

$$(x_n,y_n)=(T_n(t),U_n(t))$$

Soln:

consider,

$$\begin{aligned}
x_n+\sqrt{t^2-1}y_n &= (t+i\sqrt{1-T^2})^n \\
&= (\cos\theta+i\sqrt{1-\cos^2\theta})^n \\
&= (\cos\theta+i\sin\theta)^n \\
&= \cos n\theta+i\sin n\theta \qquad \{de\ \ Moivre's\ \ theorem\} \\
&= \cos n\arccos\theta+i\sin\arccos\theta \\
&= T_n(t)+(1-t^2)^{\frac{1}{2}}U_n(t)
\end{aligned}$$

Thus $(x_n,y_n)=(T_n(t),U_n(t))$

Q2: (a) Verify that $T_0(t)=1$, $T_1(t)=t$ & establish the recursion, for $n\geq 2$,

$$T_n(t)=2tT_n(t)-T_{n-1}(t)-T_{n-2}(t)$$

Soln:

For $n = 0$,

$T_0(t) = \cos 0 = 1$

For $n = 1$,

$T_1(t) = \cos(\arccos t) = t$

Let $t = \cos\theta$ with $0 \leq \theta \leq \pi$

We know that,

$\cos(n\theta) + \cos(n-2)\theta = 2\cos(n-1)\theta\cos\theta$

i.e $\cos((n\arccos t)) = 2\cos((n-1)\arccos t)\cos(\arccos t) - \cos((n-2)\arccos t)$

$\implies \cos(n\arccos t) = 2\cos((n-1)\arccos t)\cos(\arccos t) - \cos((n-2)\arccos t)$

$\implies T_n(t) = 2tT_n(t) - T_{n-1}(t) - T_{n-2}(t)$

(b) Use **(a)** to determine $T_2(t), T_3(t)$ & $T_4(t)$.

Soln:

For $n = 2$

$$\begin{aligned} T_2(t) &= 2tT_1(t) - T_0(t) \\ &= 2t^2 - 1 \end{aligned}$$

For $n = 3$,

$$\begin{aligned} T_3(t) &= 2tT_2(t) - T_1(t) \\ &= 2t(2t^2 - 1) - t \\ &= 4t^3 - 3t \end{aligned}$$

For $n = 4$,

$$\begin{aligned} T_4(t) &= 2tT_3(t) - T_2(t) \\ &= 2t(4t^3 - 3t) - (2t^2 - 1) \\ &= 8t^4 - 8t^2 + 1 \end{aligned}$$

Q3: (a) Verify that $U_0(t) = 0$, $U_1(t) = 1$ & establish the recursion for $n \geq 2$,

$$U_n(t) = 2tU_{n-1}(t) - U_{n-2}(t)$$

Soln:

For $n = 0$

$$U_0(t) = \frac{\sin 0}{\sin \theta} = 0$$

For $n = 1$

$$U_1(t) = \frac{\sin \theta}{\sin \theta} = 1$$

Let $t = \cos\theta$ with $0 \leq \theta \leq \pi$ and we know that,

$$\sin(n\theta) + \sin((n-2)\theta) = 2\cos\theta \sin((n-1)\theta)$$

Consider,

$$\begin{aligned} U_n(t) &= \frac{\sin(n\theta)}{\sin\theta} \\ &= \frac{2\cos\theta\sin((n-1)\theta) - \sin((n-2)\theta)}{\sin\theta} \\ &= 2\cos\theta\frac{\sin((n-1)\theta)}{\sin\theta} - \frac{\sin((n-2)\theta)}{\sin\theta} \\ &= 2tU_{n-1}(t) - U_{n-2}(t) \end{aligned}$$

(b) Use **(a)** to determine $U_2(t), U_3$ & U_4.

Soln:

For $n = 2$

$$\begin{aligned} U_2(t) &= 2tU_1(t) - U_0(t) \\ &= 2t \end{aligned}$$

For $n = 3$,

$$\begin{aligned} U_3(t) &= 2tU_2(t) - U_1(t) \\ &= 2t(2t) - 1 \\ &= 4t^2 - 1 \end{aligned}$$

For $n = 4$,

$$\begin{aligned} U_4(t) &= 2tU_3(t) - U_2(t) \\ &= 2t(4t^2 - 1) - (2t) \\ &= 8t^3 - -4t \end{aligned}$$

Q4: Prove that,

(a) $T_{2n}(t) = 1 + 2(t^2 - 1)U_n^2(t)$ for $n \geq 0$.

Soln:

$$\begin{aligned} T_{2n}(t) &= \cos 2n\theta \\ &= 1 - 2\sin^2 n\theta \\ &= 1 - 2\sin^2 \theta \left\{ \frac{\sin n\theta}{\sin \theta} \right\}^2 \\ &= 1 - 2(1 - \cos^2 \theta)U_n^2(t) \\ &= 1 - 2(1 - t^2)U_n^2(t) \\ &= 1 + 2(t^2 - 1)U_n^2(t) \end{aligned}$$

(b) $U_{2n}(t) = 2T_n(t)U_n(t)$ for $n \geq 0$.

Soln:

$$\begin{aligned} U_{2n}(t) &= \frac{\sin 2n\theta}{\sin\theta} \\ &= \frac{2\sin n\theta\cos n\theta}{\sin\theta} \\ &= 2\cos n\theta\frac{\sin n\theta}{\sin\theta} \\ &= 2T_n(t)U_n(t) \end{aligned}$$

4.5 Related Pell's Equation

In this section, we will be working on solutions when a parameter is related to other parameter for which solutions are already known.

EXERCISE:

Q1: Let d be a non square integer whose largest square divisor is m, so that $d = m^2e$ for some square square free integer e.

Prove that a Pell's equation $x^2 - dy^2 = k$ is solvable if $x^2 - ey^2 = k$ is solvable and $x^2 - ey^2 = k$ solvable if (p,q) is solution of $x^2 - dy^2 = k$ such that $m|q$.

Soln:

Suppose that $(x,y) = (r,s)$ satisfies $x^2 - dy^2 = k$

i.e $r^2 - ds^2 = k$

$\implies r^2 - (m^2e)s^2 = k$

$\implies r^2 - e(ms)^2 = k$

Thus $(x,y) = (r,ms)$ satisfies $x^2 - ey^2 = k$

Conversely,

Suppose $(x,y) = (p,q)$, where $p,q \in \mathbb{Z}$ such that $m|q \implies q = mt$

& satisfies $x^2 - ey^2 = k$

i.e $p^2 - eq^2 = k$

$\implies p^2 - em^2t^2 = k$

$\implies p^2 - dt^2 = k$

Thus $(x,y) = (p,t)$ satisfies $x^2 - dy^2 = k$.

Q2: From the smallest positive solution $(x,y) = (3,2)$ of $x^2 - 2y^2 = 1$, determine the smallest positive solution of $x^2 - dy^2 = 1$ for $d = 8$.

Soln:

For $d = 8$,

We are given that $(x,y) = (3,2)$ satisfies $x^2 - 2y^2 = 1$,

i.e $3^2 - 2(2)^2 = 1$

$\implies 3^2 - 8 = 3^2 - 8(1)^2 = 1$

Thus $(x,y) = (3,1)$ satisfies $x^2 - 8y^2 = 1$

Q3: From the solution of $(x,y) = (7,4)$ of $x^2 - 3y^2 = 1$, determine the solutions of $x^2 - dy^2 = 1$ for $d = 12$.

Soln:

Given that, $(x,y) = (7,4)$ satisfies $x^2 - 3y^2 = 1$.

i.e $7^2 - 3(4)^2 = 1$

For $d = 12$ we have,

$x^2 - 12y^2 = 1$

$\implies x^2 - 3 \times (2y)^2 = 1$

By comparing we get,

$x = 4 \quad \& \quad 2y = 4 \implies y = 2$

Thus $(x,y) = (7,2)$ satisfies $x^2 - 12y^2 = 1$.

Chapter 5

RESEARCH ARTICLES

This chapter deals with research papers which involves exponential Diophantine equation and we are interested to find it's positive integer solution, also here the Base of the exponential functions are mostly primes.

5.1 On Diophantine Equation

This section is based on paper "ON DIOPHANTINE EQUATION" by Dumitru Acu, (see [1]). In this paper Author have studied the solution in positive integer for the Diophantine equation,

$$2^x + 5^y = z^2 \tag{5.1}$$

5.1.1 Main Results:

Theorem 5.1.1.1. *The Diophantine equation, (5.1) has exactly two solutions in non negative integers, i.e* $(x,y,z) \in \{(3,0,3),(2,1,3)\}$

Proof:

Case 01: for $x = 0$

$5^y = z^2 - 1 \implies (z+1)(z-1) = 5^y$

let $z - 1 = 5^u$——(i)

and $z + 1 = 5^{y-u}$——(ii) ; where $y > 2u, u \in \mathbb{N}$

subtracting (i) from (ii) we get,

$5^{y-u} - 5^u = 2 \implies 5^u(5^{y-2u} - 1) = 2$

for u=0 we have,

$5^y - 1 = 2 \implies 5^y = 3$

This is impossible.

for $u \geq 1$ we have,

$5^u(5^{y-2u} - 1) = 2$

This is also impossible.

Case 02: for $y = 0$

$2^x = z^2 - 1 \implies (z+1)(z-1) = 2^x$

let $z - 1 = 2^v$——(iii)

and $z + 1 = 2^{x-v}$——(iv) ; where $x > 2v, v \in \mathbb{N}$

subtracting (iii) from (iv) we get,

$2^{x-v} - 2^v = 2 \implies 2^v(2^{x-2v} - 1) = 2$

for v=0 we have,

$2^x = 3$

This is impossible

for v=1 we have,

$2(2^{x-2}-1)=2$

$\implies 2^{x-2}-1=1$

$\implies 2^{x-2}=2$ Therefore for v=1, x=3 satisfies.

substitute x=3 and y=0 in (1),

$2^3+5^0=z^2$

$\implies z^2=9$

$\implies$ z=3

Therefore $(x,y,z)=(3,0,3)$ is a solution.

for $v\geq 2 \implies 2^x(2^{x-2v}-1)=2$

this is impossible.

Case 03: for $x,y\geq 1$

It follows from (1) that z is odd and not divisible by 5.

. $\therefore z\equiv \pm 1(mod5)$ or $z\equiv \pm 2(mod5)$

$\implies z^2\equiv \pm 1(mod5)$ or $z^2\equiv \pm 4(mod5)$

. $\implies z^2\equiv -1(mod5)$

To check if x is odd or even i.e x=2k or x=2k+1.

Consider,

$2^2=4\equiv -1(mod5)$

$\implies (2^2)^k\equiv (-1)^k(mod5)$

$\implies 2^{2k}\equiv (-1)^k(mod5)$

and,

$2^{2k+1}=2.2^{2k}\equiv 2.(-1)^k(mod5)$ {This is discarded}

$\therefore$ x is even

Now,

for $x = 2k$, k $\in \mathbb{N}$, (5.1) becomes,

$2^{2k} + 5^y = z^2$

$\implies z^2 - 2^{2k} = 5^y$

$\implies (z - 2^k)(z + 2^k) = 5^y$

let $(z - 2^k) = 5^w$——(v)

and $(z + 2^k) = 5^{y-w}$——(vi) ; $y > 2w, w$

subtracting (v) from (vi) we get,

$5^w(5^{y-2w} - 1) = 2^{k+1}$

for w=0,

$5^y - 2^{k+1} = 1$

if y=1

$\implies 5 - 2^{k+1} = 1$

$\implies 2^{k+1} = 2^2$

$\therefore$ for w=0 and y=1, k=1 satisfies,

$\therefore$ x=2k=2

substitute x=2 and y=1 in (5.1),

$2^2 + 5^1 = z^2$

$\implies z^2 = 9$

$\implies z = 3$

$\therefore (x, y, z) = (2, 1, 3)$ is a solution.

if $y \geq 2$,

$$5^y - 1 = 2^{k-1} \tag{5.2}$$

we show that, (5.2) has no solutions.

Sub case 01: for $y = 2l$, $l \geq 1$

Consider,

$$\begin{aligned}
5^y - 1 &= 5^{2l} - 1 \\
&= 25^l - 1 \\
&= (24+1)^l - 1 \\
&= \left[\binom{l}{0}24^l + \binom{l}{1}24^{l-1} + \cdots + \binom{l}{l-1}24 + \binom{l}{l}24^0\right] - 1 \\
&= \left[\binom{l}{0}24^l + \binom{l}{1}24^{l-1} + \cdots + \binom{l}{l-1}24\right] \\
&= 24 \times \left[\binom{l}{0}24^{l-1} + \binom{l}{1}24^{l-2} + \cdots + \binom{l}{l-1}\right] \\
&= 24C \qquad ;C = \left[\binom{l}{0}24^{l-1} + \binom{l}{1}24^{l-2} + \cdots + \binom{l}{l-1}\right]
\end{aligned}$$

$\therefore (5.2) \Longrightarrow$ 24C = 2^{k-1}

Here 3 divides L.H.S but not R.H.S.

$\therefore$ for y=2l, (A) does not have a solution.

Sub case 02: for $y = 2l+1$, $l \geq 1$

Consider,

$$\begin{aligned}
5^{2k+1}+1 &= 5^{2k+1}+1 \\
&= 5\times 25^k+1 \\
&= 5(24+1)^k+1 \\
&= 5\left[\binom{l}{0}24^l+\binom{l}{1}24^{l-1}+\cdots+\binom{l}{l-1}24+\binom{l}{l}24^0\right]+1 \\
&= 5\times 24\left[\binom{l}{0}24^{l-1}+\binom{l}{1}24^{l-2}+\cdots+\binom{l}{l-1}\right]+6 \\
&= 6\times[40\times\left[\binom{l}{0}24^{l-1}+\binom{l}{1}24^{l-2}+\cdots+\binom{l}{l-1}\right]+1] \\
&= 6K \qquad ;K=\left[40[\binom{l}{0}24^{l-1}+\binom{l}{1}24^{l-2}+\cdots+\binom{l}{l-1}\right]+1]
\end{aligned}$$

Now suppose,

$$\begin{aligned}
2^{k+1} &= 5^y-1 \\
&= 5^{2l+1}-1 \\
&= (5-1)[5^{2l}+5^{2l-1}+5^{2l-2}+5^{2l-3}+\cdots+5^3+5^2+5+1] \\
&= 4\times[(5^{2l}-1)+(5^{2(l-1)+1}+1)+(5^{2(l-1)}-1)+\cdots+(5^2-1)+(5+1)+1] \\
&= 4\times[24C_1+6K_1+24C_2+6K_2+\cdots+24+6+1]
\end{aligned}$$

$$\begin{aligned}
\implies 2^{k-1} &= 24C_1+6K_1+24C_2+6K_2+\cdots+24+6+1 \\
&= 6(4C_1+K_1+4C_2+K_2+\cdots+4+1)+1 \\
&= 6N+1 \qquad ;N=4C_1+K_1+4C_2+K_2+\cdots+4+1
\end{aligned}$$

here L.H.S is even but R.H.S is odd.

$\therefore$ for y=2l+1, (A) does not have a solution.

hence the equation $5^y - 1 = 2^{k-1}$ does not have a solution for $y > 1$

In conclusion, The Diophantine equation $2^x + 5^y = z^2$ has exactly two non negative integer solutions, i.e $(x, y, z) \in \{(3,0,3),(2,1,3)\}$.

5.2 On Diophantine Equation $7^x + 8^y = z^2$

This section is based on the paper "ON DIOPHANTINE EQUATION $7^x + 8^y = z^2$" by Banyat Sroysang (see [8]). In this paper, Author have shown that the Diophantine equation $7^x + 8^y = z^2$ has a unique non-negative integer solution and is given by $(x, y, z) = (0,8,3)$.

5.2.1 Preliminaries:

Lemma 5.2.1.1. *The diophantine equation $7^x + 1 = z^2$ has no non-negative integer solution.*

Proof:

Suppose to the contrary there are non-negative integers x and z such that $7^x + 1 = z^2$.

if $x = 0$

$\implies 7^0 + 1 = z^2$

$\implies 2 = z^2$

This is impossible.

if $x = 1$

$\implies 7^1 + 1 = z^2$

$\implies 8 = z^2$

This is impossible.

if $x \geq 2$

$\implies 7^x + 1 = z^2$

$\implies 7^x = z^2 - 1$

$\implies 7^x = (z+1)(z-1)$

$\therefore z+1 = 7^{x-s}$ & $z-1 = 7^s$ for some $s \in \mathbb{Z}$ such $x > 2s, s$

Subtracting above eqns we get,

$7^{x-s} - 7^s = 2$

$\implies 7^s(7^{x-2s} - 1) = 2$

If $s = 0$, then $7^x - 1 = 2$.

For any $x \in \mathbb{Z}$ (even or odd)

$(7-1)(7^{x-1} + 7^{x-2} + \cdots + 1) = 2$

$6(7^{x-1} + 7^{x-2} + \cdots + 1) = 2$

This is contradiction as 3 divides L.H.S but not R.H.S

If $s \geq 1$, then $7^s(7^{x-2s} - 1) = 2$.

This is contradiction as 7 divides L.H.S but not R.H.S

Hence the eqn $7^x + 1 = z^2$ has no non-negative integer solution.

Lemma 5.2.1.2. $(1,3)$ *is a unique solution* (y,z) *for the Diophantine equation* $1+8^y = z^2$ *where y and z are non-negative integers.*

Proof:

Let $y\&z$ be non negative intergers such that $1+8^y = z^2$

If $y = 0$ then,

$1+8^0 = z^2$

$\implies 2 = z^2$,which is impossible

If $y = 1$ then,

$1+8^1 = z^2$

$\implies 9 = z^2$

$\implies z = 3$ since we are looking for non negative solutions.

$\therefore (1,3)$ is a solution.

If $y \geq 2$ then,

$1+8^y = z^2$

$\implies 8^y = z^2 - 1$

$\implies 8^y = (z-1)(z+1)$

$\implies z-1 = 8^k$ & $z+1 = 8^{y-k}$ $k \in \mathbb{Z}$ such that $y > 2k, k$

subtracting above equations we get,

$8^{y-k} - 8^k = 2$

$\implies 8^k(8^{y-2k} - 1) = 2$

If $t = 0$ then,

$8^y - 1 = 2$,

this is impossible since L.H.S is odd & R.H.S is even.

If $t \geq 1$ then,

$8^{y-k} - 8^k = 2$

this is also impossible since L.H.S is divisible by 8 but not R.H.S.

Hence $1 + 8^y = z^2$ has a unique solution i.e $(y,z) = (1,3)$

5.2.2 Main Results:

Lemma 5.2.2.1. $(0,1,3)$ *is a unique solution* (x,y,z) *for the diophantine equation* $7^x + 8^y = z^2$*, where* x,y *&* z *are non negative integers.*

Proof:

Let x,y & z are non negative integers such that $7^x + 8^y = z^2$.

By lemma 1, we see that $7^x + 1 = z^2$ has no non negative integer solution.

$\therefore y \neq 0$

Hence $y \geq 1$

Now for number x,

Case 01: $x = 0$

$1 + 8^y = z^2$

By lemma 2, $(y,z) = (1,3)$ is the unique solution.

$\therefore (x,y,z) = (0,1,3)$ is a solution.

Case 02: $x \geq 1$

It is clear that z is odd.

$\therefore z^2 \equiv 1 (\text{mod } 4)$

$\implies 7^x \equiv 1 (\text{mod } 4)$

Thus x is even.

Let $x = 2k$; $k \in \mathbb{N}$, then,

$7^{2k} + 8^y = z^2$

$\implies z^2 - 7^{2k} = 8^y$

$(z - 7^k)(z + 7^k) = 8^y$

Thus $z - 7^k = 8^u$ & $z + 7^k = 8^{y-u}$,where $u \in \mathbb{Z}$ such that $y > 2u, u$

Subtracting above equations we get,

$$\begin{aligned} 2(7^k) &= 8^{y-u} - 8^u \\ &= 8^u(8^{y-2u} - 1) \end{aligned}$$

For $u = 0$,

$2(7^k) = 8^y - 1$

This is impossible since L.H.S is even & R.H.S is odd.

For $u \geq 1$

$2(7^k) = 8^u(8^{y-2u} - 1)$

This is impossible since 8 divides R.H.S but not L.H.S.

Hence $(x, y, z) = (0, 1, 3)$ is a unique solution for equation $7^x + 8^y = z^2$, where x, y & z are non negative integers.

Corollary 5.2.2.2. *The diophantine equation* $7^x + 8^y = w^4$ *has no non negative integer solution.*

Proof:

Suppose that $\exists$ a non negative integer solution for $7^x + 8^y = w^4$ for integers x, y & w.

Let $z = w^2$, then

$7^x + 8^y = z^2$

By above theorem this equation has a unique solution given by $(x, y, z) = (0, 1, 3)$.

$\therefore z = 3$

$\implies w^2 = 3$

$\implies w = \sqrt{3} \notin \mathbb{N} \bigcup \{0\}$

Hence the equation $7^x + 8^y = w^4$ has no non negative integer solution.

5.3 On Diophantine Equation $p^x + (p+1)^y = z^2$, where p is Mersenne Prime

This section is based on the paper "ON DIOPHANTINE EQUATION $p^x + (p+1)^y = z^2$" by Somchit Chotchaisthit (see [3]). In this paper, Author have shown that $(p, x, y, z) \in \{(7, 0, 1, 3), (3, 2, 2, 5)\}$ are the only solutions of Diophantine equation $p^x + (p+1)^y = z^2$, where x, y, z are non-negative integers and p is a Mersenne prime.

5.3.1 Preliminaries:

A Mersenne number is a number of the form $2^n - 1$, where n is a positive integer. If Mersenne number is a prime, then it is called Mersenne prime. In order for $2^n - 1$ to be prime, n should also be a prime. This is true since for a composite $n = rs$, $r,s \in \mathbb{N}$ $2^n - 1 \implies 2^{rs} - 1$, which is a binomial number having factors.

5.3.2 Main Results:

Theorem 5.3.2.1. *The Diophantine equation, $p^x + (p+1)^y = z^2$ where p is a Mersenne prime, has only two solutions, namely $(p,x,y,z) \in \{((7,0,1,3),(3,2,2,5)\}$.*

Proof:

Let p be a Mersenne prime, then $p = 2^q - 1$ for some prime q.

Here p is odd, hence p^x is odd and $(p+1)$ is even, hence $(p+1)$ is even.

$\implies z$ is odd & is given by $z^2 \equiv 1(\text{mod } 4)$

Now,

$\because p = 2^q - 1 \quad ,q \geq 2$

$$\begin{aligned} \implies p &\equiv (2^q - 1)(mod 4) \\ &\equiv (0-1)(mod 4) \\ &\equiv -1(mod 4) \\ &\equiv 3(mod 4) \end{aligned}$$

$$\begin{aligned} \&(p+1) &\equiv (3+1)(mod 4) \\ &\equiv 0(mod 4) \end{aligned}$$

Now consider the Diophantine equation,

$$p^x + (p+1)^y = z^2 \text{ ——(1)}$$

Case 01: Suppose $x = 0$, then (1) becomes,

$1 + (p+1)^y = z^2$

$\implies (p+1)^y = z^2 - 1$

$\implies 2^{qy} = (z-1)(z+1)$

Hence $\exists$ non-negative integers α, β such that, $2^\alpha = (z+1)$ & $2^\beta = (z-1)$, where $\alpha > \beta$ & $\alpha + \beta = qy$.

Subtracting above equations we get,

$2^\alpha - 2^\beta = (z+1) - (z-1)$

$\implies 2^\beta(2^{\alpha-\beta} - 1) = 2p^k$

Here, If $\beta = 0$, then L.H.S will be odd and R.H.S will be even, $\therefore \beta \neq 0$.

also, If $\beta > 1$, then L.H.S will be divisible by 4 (at least) and R.H.S will only be divisible by 2, $\therefore \beta \not> 1$.

$\therefore \beta = 1$

$\therefore (1) \implies 2(2^{\alpha-1} - 1) = 2$

$\implies 2^{\alpha-1} - 1 = 1$

$\implies 2^{\alpha-1} = 2$

$\therefore \alpha = 2$

$\because \alpha + \beta = 3 = qy$ & q is a prime we have,

$q = 3$ & $y = 1$

$\therefore p = 2^q - 1 = 8 - 1 = 7$

Substituting $p = 7$, $x = 0$, & $y = 1$ in (1) we get $z = 3$

$\therefore (p, x, y, z) = (7, 0, 1, 3)$ is a solution of (1).

Case 02: Suppose $x \geq 1$

Here we have $(p+1)^y \equiv 0 (\text{mod } 4)$ & $z^2 \equiv 1 (\text{mod } 4)$

$\implies p^x \equiv 3(\text{mod } 4)$

$\therefore x$ must be even, i.e $x = 2k$, for integer $k \geq 1$

Hence we have,

$$p^{2k} + (p+1)^y = z^2$$
$$\implies 2^{qy} = z^2 - p^{2k}$$
$$= (z - p^k)(z + p^k)$$

Thus $\exists$ non-negative integers α, β such that,

$2^\alpha = z + p^k \quad \& \quad 2^\beta = z - p^k$, where $\alpha > \beta \quad \& \quad \alpha + \beta = qy$

Subtracting above equations we get,

$2^\beta(2^{\alpha-\beta} - 1) = 2p^k$

Here, if $\beta = 0$ then L.H.S is odd and R.H.S is even $\therefore \beta \neq 0$

Also if $\beta > 1$ then L.H.S is at least divisible by 4 but R.H.S is only divisible by 2, $\therefore \beta \not> 1$.

For $\beta = 1$ & $(\alpha - 1), k > 1$ we have,

$2^{\alpha-\beta} - 1 = p^k$ ———(2)

$$\implies 2^{\alpha-\beta} = p^k + 1$$
$$= (2^q - 1)^k + 1$$
$$= \left[\binom{k}{0}(2^q)^k - \binom{k}{1}(2^q)^{k-1} + \cdots + (-1)^{k-1}\binom{k}{k-1}(2^q) + (-1)^k\binom{k}{k}1\right] + 1$$

Here, if k is even,

$$2^{\alpha-\beta} = \binom{k}{0}(2^q)^k - \binom{k}{1}(2^q)^{k-1} + \cdots + (-1)^{k-1}\binom{k}{k-1}(2^q) + 1 + 1$$
$$= \binom{k}{0}(2^q)^k - \binom{k}{1}(2^q)^{k-1} + \cdots + (-1)^{k-1}\binom{k}{k-1}(2^q) + 2$$

$\therefore 2^{\alpha-\beta} = 2\left[\binom{k}{0}(2^{q+k-1} - \binom{k}{1}(2^{q+k-2} + \cdots + (-1)^{k-1}\binom{k}{k-1}(2^{q-1}) + 1\right]$

There's a contradiction $\because$ every component on L.H.S is even but there's an odd component on R.H.S.

Now, if k is odd,

$$\begin{aligned} 2^{\alpha-\beta} &= \binom{k}{0}(2^q)^k - \binom{k}{1}(2^q)^{k-1} + \cdots + (-1)^{k-1}\binom{k}{k-1}(2^q) - 1 + 1 \\ &= 2^q\left[\binom{k}{0}(2^q)^{k-1} - \binom{k}{1}(2^q)^{k-2} + \cdots + (-1)^{k-1}k\right] \end{aligned}$$

Again there's a contradiction $\because$ every component on L.H.S is even but there's an odd component on R.H.S {as k is odd.}.

$\therefore (\alpha - 1) = 0 \quad$ or $\quad k = 1$

Suppose for $\beta = 1$ we choose $k = 1$

$$\begin{aligned} \textit{then } (2) &\implies 2^{\alpha-1} - 1 = p \\ &\implies 2^{qy-2} - 1 = 2^q - 1 \qquad \{\because \alpha + \beta = qy \implies \alpha = qy - 1\} \\ &\implies qy - 2 = q \\ &\implies q(y-1) = 2 \\ &\implies q = 2 \quad \& \quad (y-1) = 1 \quad \therefore y = 2 \end{aligned}$$

$\implies p = 2^q - 1 = 3 \quad \& \quad x = 2k = 2$

$$\begin{aligned} \therefore z^2 &= p^x + (p+1)^y \\ &= 3^2 + 4^2 \\ &= 25 \end{aligned}$$

$\implies z = 5$

$\therefore (p,x,y,z) = (3,2,2,5)$ is the solution to (1).

Suppose for $\beta = 1$ we choose $(\alpha - 1) = 1$

$$\begin{aligned} then\ (2) \implies p &= 2^{\alpha-1} - 1 \\ &= 2^1 - 1 \\ &= 1 \end{aligned}$$

$\implies k = 0$, which is contradiction to the fact that $k \geq 1$, hence (1) has no solutions in this case.

$\therefore$The solutions of Diophantine equation $p^x + (p+1)^y = z^2$ are,

$(p,x,y,z) \in \{((7,0,1,3),(3,2,2,5)\}$.

Author concluded with the note that he found the solution for p being a Mersenne prime and the Diophantine equation $p^x + (p+1)^y = z^2$ where p is not a Mersenne prime remains an open problem.

5.4 Complete Set of Solutions of the Diophantine Equation $p^x + q^y = z^2$ for Twin Primes p & q

This section is based on the paper "COMPLETE SET OF SOLUTIONS OF THE DIOPHANTINE EQUATION $p^x + q^y = z^2$ FOR TWIN PRIMES p & q" by Jerico B. Bacani1, Julius Fergy T. Rabago (see [6]). In this paper, Author have shown that the Diophantine equation.

$$p^x + q^y = z^2 \tag{5.3}$$

infinitely many solution using twin prime conjecture. Author's main purpose was to correct the result of A. Suvarnamani who claimed that (5.3) has a unique solution in [10].

5.4.1 Preliminaries:

Lemma 5.4.1.1. *Let $q > p > 3$ be twin primes, then $12|(p,q)$.*

Proof:

Let p & q be twin primes such that $p > 3$.

$\because$ any 2 twin primes greater than 3 are of the form,

$$6l-1 \quad \& \quad 6l+1 \qquad ; l \in \mathbb{N}$$

and we are given that $q > p$ we have,

$$p = 6l-1 \quad \& \quad q = 6l+1$$

It follows that $p+q = 12l$

$\implies 12|(p+q)$

Lemma 5.4.1.2. *Let $q > p > 3$ be twin primes, then (1) has infinitely many solutions in $\mathbb{N}$ of the form $(p,q,x,y,z) = (6(3l^2)-1, 6(3l^2)+1, 1, 1, 6l)$, where $l \in \mathbb{N}$.*

Proof:

We first assume that the twin prime conjecture is true.

Also, $\because$ twin primes are expressed as $6l-1$ & $6l+1$, We take $l \to 3l$

Thus we have,

$$\begin{aligned} p+q &= 6(3l^2)-1+6(3l^2)+1 \\ &= 36l^2 \end{aligned}$$

Thus, if $p = 6(3l^2)-1$ & $q = 6(3l^2)+1$ are twin primes then,

$(p,q,x,y,z) = (6(3l^2)-1, 6(3l^2)+1, 1, 1, 6l)$ is a solution to $p^x + q^y = z^2$.

So if there exist an infinite pair of twin primes (p,q) of such kind, then there also exist an infinite number of solutions (p,q,x,y,z) to (1) in $\mathbb{N}$

REMARK:

We note that even if $q=p+2$ is not a prime, the equation (1) still has infinitely many solutions (p,q,x,y,z) in $\mathbb{N}$ of the form, $(6(3l^2)-1,6(3l^2)+1,1,1,6l)$ where $l\in\mathbb{N}$.

Lemma 5.4.1.3. *The Diophantine equation $1+p^x=z^2$, where p is an odd prime has exactly two solution (p,q,z) in $\mathbb{N}\bigcup\{0\}$, namely $(3,1,2)$ & $(2,3,3)$.*

Proof:

It suffices to assume that $x>0$ $\because z^2=2$ is impossible.

If $x\geq 1$, then

$1+p^x=z^2$

$\implies p^x=(z-1)(z+1)$

$\implies (z-1)=p^\alpha \quad \& \quad (z+1)=p^\beta$

where $\alpha,\beta\in\mathbb{Z}$, $\alpha>\beta$ & $\alpha+\beta=x$

$\implies p^\alpha-p^\beta=(z+1)-(z-1)$

$\implies p^\beta(p^{\alpha-\beta}-1)=2$

If $\beta=0$, we have,

$p^\alpha-1=2$

i.e $p^\alpha=3$

$\therefore p=3$ & $\alpha=1$ hence $x=1$

Substituting $p=3$ & $x=1$ in $1+p^x=z^2$, we get $z=2$.

Thus $(p,q,z)=(3,1,2)$ is a solution.

If $\beta=1$, we have,

$\because p$ is a prime $p=2$ & $p^{\alpha-1}-1=1 \implies 2^{\alpha-1}=2$

$\therefore \alpha = 2$ and hence $x = 3$

Substitute $p = 2$ & $x = 3$ in $1 + p^x = z^2$, we get $z = 3$,

Thus $(p,q,z) = (2,3,3)$ is a solution.

REMARK:

It is stated in {[10] lemma 2.2} that, *If q is an odd prime number & y,z are non negative integers, then the Diophantine equation $1 + q^y = z^2$ has no solutions.* We remark this statement is only true provided q is assumed to be prime greater than 3.

Lemma 5.4.1.4. *Let p & q be fixed twin primes, then equation (1) is never possible for $min\{x,y\} > 1$.*

Proof:

Let p & q be twin primes.

Then there are two cases,

First suppose that $p \equiv 1(\text{mod } 4)$ & $q \equiv -1(\text{mod } 4)$, then x,y must be of opposite parity and z is even.

so we consider two sub possibilities.

(i) x is even & y is odd.

If $x = 2k$ for some $k \in \mathbb{N}$, then

$q^y = (z + p^k)(z - p^k)$

$\implies z + p^k = q^\beta$ & $z - p^k = q^\alpha$; where $\alpha, \beta \in \mathbb{Z}$, $\alpha < \beta$ & $\alpha + \beta = y$

$\implies 2p^k = q^\alpha(q^{\beta-\alpha} - 1)$

$\because q \neq 2, p \implies \alpha = 0$

$\therefore 2p^k = (q^\beta - 1)$

Note that, if $p \equiv 1(\text{mod } 4)$ then $p \equiv -1(\text{mod } 6)$ & $2p^k \equiv 1,2(\text{mod } 3)$.

Furthermore, $\because q \equiv 1(\text{mod } 6)$ & $q^\beta - 1 \equiv 0(\text{mod}3)$ whenever $q \equiv -1(\text{mod}4)$
then $2p^k \not\equiv (q^\beta - 1)(\text{mod } 3)$

(ii) y is even & x is odd.
If $y = 2l$ for some $l \in \mathbb{Z}$, then
$p^x = (z+q^l)(z-q^l)$
$\implies z+q^l = p^\beta$ & $z-q^l = p^\alpha$; where $\alpha, \beta \in \mathbb{Z}$, $\alpha < \beta$ & $\alpha+\beta = x$
$\implies 2q^l = p^\alpha(p^{\beta-\alpha}-1)$
$\because p \neq 2, q \implies \alpha = 0$
$\therefore 2q^l = (p^\beta - 1)$
Note that, if $q \equiv -1(\text{mod } 4)$ then $2q^l \equiv 2(\text{mod } 4)$.
Also, $\because p^\beta \equiv 1(\text{mod } 4) \implies p^\beta - 1 \equiv 0(\text{mod } 4)$
then $2q^l \not\equiv (p^\beta - 1)(\text{mod } 4)$

Now, suppose that $p \equiv -1(\text{mod } 4)$ & $q \equiv 1(\text{mod } 4)$, then again x, y are of opposite parity & z is even.
If $x = 2k$ for some $k \in \mathbb{N}$, then
$q^y = (z+p^k)(z-p^k)$
$\implies 2q^k = q^y - 1$
so $2p^k \equiv 2(\text{mod } 4)$ & $q^y - 1 \equiv 0(\text{mod } 4)$
$\implies 2p^k \not\equiv q^y - 1(\text{mod } 4)$

Similarly,
If $y = 2l$, then we get $2q^l = p^\beta - 1$
$\because 2q^l \equiv 2(\text{mod } 6)$ & $p^\beta - 1 \equiv 4(\text{mod } 6)$
$\implies 2q^l \not\equiv p^\beta - 1(\text{mod } 6)$

We have shown that if p & q are twin primes, then the equation (1) has no solutions (x,y,z) in $\mathbb{N}$. This proves the Lemma.

5.4.2 Main Results:

Theorem 5.4.2.1. *Let p & q be fixed twin primes & their sum be a perfect square, then the equation (5.3) has the unique solution $(x,y,z) = (1,1,\sqrt{p+q})$.*

Proof:

Let p & q be twin primes.

w.l.o.g, we assume that $p < q$.

by assumption, the sum of p & q is a perfect square.

clearly, $p \geq 17$ & $q \geq 19$

$\therefore (x,y,z) = (1,1,\sqrt{p+q})$ is a solution to $p^x + q^y = z^2$.

Now **T.S.T:** The solution (x,y,z) of $p^x + q^y = z^2$ is unique.

It suffices to assume that $min\{x,y\} > 1$.

From Lemma 02, we see that p & q are of different residue classes modulo 4.

i.e if $p \equiv 1,-1 \pmod 4$, then $q \equiv -1,1 \pmod 4$ respectively.

Using Lemma 03 & Lemma 04, we obtain no solution (x,y,z) to $p^x + q^y = z^2$ in $\mathbb{N}\bigcup\{0\}$ except $(1,1,\sqrt{p+q})$.

This proves the main result.

A consequence of our main result is given in next corollary.

Corollary 5.4.2.2. *Let p & q be fixed such that p,q are twin primes. then, the Diophantine equation $p^x + q^y = z^2$ has at most one solution in $\mathbb{N}\bigcup\{0\}$.*

We have the following table for some particular values of p & q,

$p^x + q^y = z^2$	**Unique solution in $\mathbb{N} \bigcup \{0\}$**
$881^x + 883^y = z^2$	(1,1,42)
$1151^x + 1153^y = z^2$	(1,1,48)
$2591^x + 2593^y = z^2$	(1,1,72)
$3527^x + 3529^y = z^2$	(1,1,84)
$4049^x + 4051^y = z^2$	(1,1,90)

5.5 On Diophantine Equation $p^x + (p+1)^y = z^2$

In this section, the paper "ON DIOPHANTINE EQUATION $p^x + (p+1)^y = z^2$" by Alongkat Suvarnamani (see [9]), have claimed that the Diophantine equation $p^x + (p+1)^y = z^2$ have a unique solution. But we see that for prime p which is 2 less than being perfect square is also a solution. We will look at these solutions in this section.

5.5.1 Main Results:

Theorem 5.5.1.1. *For a Diophantine equation,*

$$p^x + (p+1)^y = z^2 \quad \text{——(1)}$$

where p is an odd prime number & $x,y,z \in \mathbb{N} \bigcup \{0\}$, then $(p,x,y,z) = (3,1,0,2)$ or $(p,x,y,z) = (p,0,1,n)$ if $p = n^2 - 2$ is a solution of (1).

Proof:

Let p be an odd prime & $x,y,z \in \mathbb{N}\bigcup\{0\}$, then for (1) we have 3 cases as follows:

Case 01: Suppose $x = 0$,

Then (1) $\Longrightarrow\ 1+(p+1)^y = z^2$

Here we have 3 sub cases:

sub case 01: For $y = 0$ we have,

$z^2 = 2$, which is impossible.

sub case 02: For $y = 1$

$z^2 = p+2$

$\therefore$ There are primes that are 2 less than a perfect square {**eg.**7,23,79,...}

$\therefore (p,x,y,z) = (p,0,1,n)$ are solutions of (1), where p is a prime of a type $p = n^2-2$; $n \in \mathbb{N}$

sub case 03: For $y > 1$

$z^2 = (p+1)^y + 1$

$\Longrightarrow\ (p+1)^y = (z-1)(z+1)$

$\therefore (z-1) = (p+1)^\alpha\ \ \&\ \ (z+1) = (p+1)^\beta$,

where $\alpha,\beta \in \mathbb{Z},\quad \beta > \alpha \quad \& \quad \alpha+\beta = y$

$\therefore (p+1)^\alpha[(p+1)^{\beta-\alpha}-1] = 2$

If $\alpha > 0$ then L.H.S is divisible by $(p+1)$ but not R.H.S, $\therefore \alpha = 0$.

$\Longrightarrow\ (p+1)^\beta - 1 = 2$

$\Longrightarrow\ (p+1)^\beta = 3$

This is impossible, $\because$ only possible case is if $p = 2$ & $\beta = 1$ but p is odd prime.

Case 02: Suppose $y = 0$,

Then (1) $\Longrightarrow\ p^x + 1 = z^2$

Here also we have 3 sub cases:

sub case 01: For $x = 0$

$z^2 = 2$, which is impossible.

sub case 02: For $x = 1$

$z^2 = p + 1$

And we know that only prime that's 1 less than being a perfect prime is 3.

$\therefore p = 3 \quad \& \quad z = 2.$

Hence $(p, x, y, z) = (3, 1, 0, 2)$ is a solution of (1).

sub case 03: for $x > 1$

$z^2 = p^x + 1$

$\implies p^x = z^2 - 1$

$\therefore (z-1) = p^m \quad \& \quad (z+1) = p^n,$ where $m, n \in \mathbb{Z}, \quad n > m \quad \& \quad m + n = x$

$\therefore p^m(p^{n-m} - 1) = 2$

clearly, $m = 0$

$\implies p^n - 1 = 2$

$\implies p^n = 3$

Thus $p = 3 \quad \& \quad n = 1 \implies x = 1$

But this contradicts the fact that $x > 1$.

Case 03: Suppose $x, y \geq 1$

$$p^x + (p+1)^y = z^2$$

Clearly z is odd $\therefore z^2 \equiv 1 (\text{mod } 4)$ & $(p+1)$ is even $\therefore (p+1)^y \equiv 0 (\text{mod } 4)$,

Hence $p^x \equiv 1(\text{mod } 4) \implies x$ is even i.e $x = 2k$ for $k \in \mathbb{Z}^+$

$$\therefore (p+1)^y = (z-p^k)(z+p^k)$$
$$\implies (z-p^k) = (p+1)^u \ \& \ (z+p^k) = (p+1)^v \quad ; u,v \in \mathbb{Z},\ v > u \ \& \ u+v = y$$
$$\implies (p+1)^u[(p+1)^{v-u} - 1] = 2p^k$$
$$\because p+1 \neq 2, p \implies u = 0$$

Thus $(p+1)^v - 1 = 2p^k$

This is also not possible $\because$ L.H.S is odd & R.H.S is even.

$\therefore (p,x,y,z) = (3,1,0,2)$ or $(p,x,y,z) = (p,0,1,n)$ if $p = n^2 - 2$ is a solution of (1).

Remark: 5.5.1.2. *If p is even prime i.e $p = 2$ then,*

$$(1) \implies 2^x + 3^y = z^2 \text{ ———(2)}$$

Here we have 3 cases as follows:

case 01: For $x = 0$ we have,

$1 + 3^y = z^2$

$\implies 3^y = (z-1)(z+1)$

$\implies 3^\alpha = (z-1)$ & $3^\beta = (z+1)$

$\implies 3^\alpha(3^{\beta-\alpha} - 1) = 2$

$\implies \alpha = 0$

$\therefore 3^\beta - 1 = 2$

$\implies 3^\beta = 3$

$\therefore \beta = 1$

$\therefore y = 1$ & $z = 2$

$\therefore (p,x,y,z) = (2,0,1,2)$ is a solution of (2)

case 02: For $y = 0$ we have,

$2^x + 1 = z^2$

$\implies 2^x = (z-1)(z+1)$

$\implies 2^m = (z-1)$ & $2^n = (z+1)$

$\implies 2^m(2^{n-m} - 1) = 2$

$\implies m = 1$

$\therefore 2^{n-1} - 1 = 1$

$\implies 2^{n-1} = 2$

$\therefore n = 2$

Thus $x = 3$ & $z = 3$

$\therefore (p,x,y,z) = (2,3,0,3)$ is a solution of (2).

case 03: For $x, y \geq 1$

From (2), it is clear that z is not divisible by 3.

$\therefore z \equiv \pm 1 (\text{mod } 3) \implies z^2 \equiv 1 (\text{mod } 3)$

Also,

$2^2 = 4 \equiv 1 (\text{mod } 4)$

$\implies (2^2)^k \equiv 2^{2k} \equiv 1 (\text{mod } 3)$

But $2^{2k+1} \equiv 2 (\text{mod } 3) \equiv -1 (\text{mod } 3)$

$\therefore x$ is even i.e $x = 2k$, for $k \in \mathbb{Z}$.

$\therefore 3^y = (z - 2^k)(z + 2^k)$

$\implies 3^u = z - 2^k \quad \& \quad 3^v = z + 2^k \quad ; u, v \in \mathbb{Z},\ v > u \ \&\ u + v = y$

$\implies 3^u(3^{v-u} - 1) = 2(2^k) = 2^{k+1}$

$\therefore u = 0$

$\implies 3^v - 1 = 2^{k+1}$

$\therefore v = 2 \quad \& \quad k = 2$ satisfies the equation.

Thus $y = 2$ & $x = 4$

Substituting $y = 2$ & $x = 4$ in (2) we get $z = 5$

$\therefore (p,x,y,z) = (2,4,2,5)$ is a solution of (2)

Also note that,

putting $(p,x,y,z) = (2,4,2,5)$ in (1) we get,

$2^4 + 3^2 = 5^2$ which can also be written as $4^2 + 3^2 = 5^2$

$\therefore$ For $p = 3$, we have (p+1)=4

Thus $(p,x,y,z) = (3,2,2,5)$ is also a solution of (1).

Chapter 6

ANALYSIS AND CONCLUSIONS

In **Chapter 2 & 3** includes the textbook data. We have determined the solutions for some of the Quadratic Diophantine equations and Linear Diophantine equations. I have done a detailed proof of all the results and included all steps that were missing in books [7] & [5].

In **Chapter 4** we look at Pell's equation. We learn the relation between Quadratic surds and Pell's equation. We see that if we are given a integer solution we can find a rational solution and vice versa. We can also find recursive solutions of surds if surds can be expressed in terms of powers. We also see role of Chebyshev polynomials in this section. Lastly we find solutions of Pell's equations whose parameter are related other equation whose solution is already known.

And **Chapter 5** is based research articles. The all authors of the articles have used a result, *Catalan's conjecture* but in my report I have not used *Catalan's conjecture* and proved the result by manual calculation. Also in the last section, We see that the Diophantine equation $p^x + (p+1)^y = z^2$ than in [9] where p is an odd prime have

solutions of the form $(x,y,z) = (0,1,n)$ for prime p of the form $p = n^2 - 2$ where $n \in \mathbb{N}$ and found solutions for only even prime $p = 2$.

Bibliography

[1] Dumitru Acu. "On a diophantine equation1". In: *General Mathematics* 15 (Jan. 2007).

[2] E.J. Barbeau. *Pell's Equation*. Problem Books in Mathematics. Springer New York, 2006. ISBN: 9780387226026. URL: https://books.google.co.in/books?id=jzLTBwAAQBAJ.

[3] Somchit Chotchaisthit. "ON THE DIOPHANTINE EQUATION $p^x+(p+1)^y=z^2$ WHERE p IS A MERSENNE PRIME". In: *International Journal of Pure and Apllied Mathematics* 88 (Oct. 2013). DOI: 10.12732/ijpam.v88i2.2.

[4] L.J. Mordell. *Diophantine equations: Diophantine Equations*. ISSN. Elsevier Science, 1969. ISBN: 9780080873428. URL: https://books.google.co.in/books?id=QugvF7xfE-oC.

[5] I. Niven and H.S. Zuckerman. *An Introduction to the Theory of Numbers*. Wiley, 1972. ISBN: 9780471641544. URL: https://books.google.co.in/books?id=ez43W5xlv5wC.

[6] Julius Fergy Rabago and Jerico Bacani. "THE COMPLETE SET OF SOLUTIONS OF THE DIOPHANTINE EQUATION $\mathrm{p}^x+q^y=z^2 FORTWINPRIMESpANDq$". In: *International Journal of Pure and Applied Mathematics* 104 (Nov. 2015), pp. 517–. DOI: 10.12732/ijpam.v104i4.3.

[7] D. Redmond. *Number Theory: An Introduction to Pure and Applied Mathematics*. CRC Press, 2020. ISBN: 9781000148572. URL: https://books.google.co.in/books?id=s_j_DwAAQBAJ.

[8] B. Sroysang. "ON THE DIOPHANTINE EQUATION $7^x + 8^y = z^2$". In: *International Journal of Pure and Apllied Mathematics* 84 (Apr. 2013). DOI: 10.12732/ijpam.v84i1.8.

[9] Alongkot Suvarnamani. "ON THE DIOPHANTINE EQUATION $p^x + (p+1)^y = z^2$". In: *International Journal of Pure and Apllied Mathematics* 94 (Aug. 2014). DOI: 10.12732/ijpam.v94i5.5.

[10] Alongkot Suvarnamani. "SOLUTION OF THE DIOPHANTINE EQUATION $p^x + q^y = z^2$". In: *International Journal of Pure and Apllied Mathematics* 94 (Aug. 2014). DOI: 10.12732/ijpam.v94i4.1.