DIOPHANTINE EQUATIONS

A project report submitted to Mahatma Gandhi University in partial fulfilment of the requirements of the award of Bachelor's Degree in Mathematics.

Submitted by,

DEVIKA SANTHOSH (180021035904)

DONA JOSE (180021035906)

ELJA GEORGE (180021035909)

VINAYAK KANNAN (180021035939)

Department of Mathematics

NIRMALA COLLEGE MUVATTUPUZHA

2018-2021

Mr. Saji Joseph

Head of the Department

Department of Mathematics

Nirmala College, Muvattupuzha

CERTIFICATE

This is to certify that work entitled **"DIOPHANTINE EQUATIONS"** is a bonafide record of the work done by **DEVIKA SANTHOSH (180021035904), DONA JOSE (180021035906) , ELJA GEORGE (180021035909) ,VINAYAK KANNAN (180021035939)** of Nirmala College, Muvattupuzha under the supervision and guidance of **Mr. Arun George**, Guest Lecturer on contract, Department of Mathematics, in partial fulfilment of the requirements for the award of Bachelor's Degree in Mathematics of Mahatma Gandhi University, Kottayam.

Mr. Saji Joseph

Head of the Department

PLACE: MUVATTUPUZHA

DATE:

Mr. Arun George

Guest Lecturer on contract

Department of Mathematics

Nirmala College, Muvattupuzha

CERTIFICATE

This is to certify that work entitled **"DIOPHANTINE EQUATIONS"** submitted in partial fulfilment of the requirements for the award of Bachelor's Degree in Mathematics of Mahatma Gandhi University ,Kottayam is a bonafide record of the work done by **DEVIKA SANTHOSH (180021035904), DONA JOSE (180021035906) , ELJA GEORGE (180021035909) ,VINAYAK KANNAN (180021035939)** in the Department of Mathematics , Nirmala College Muvattupuzha under my supervision and guidance , during the year, 2018-2021.

Mr. Arun George

PLACE: MUVATTUPUZHA

DATE:

DECLARATION

We hereby declare that the project report entitled **"DIOPHANTINE EQUATIONS"** submitted in partial fulfilment of the requirements for the award of the Degree of Bachelor in Mathematics of Mahatma Gandhi University, Kottayam is our destination work. The contents of the study, in full or parts have not been submitted to any other institution or any university for the award of any degree or diploma.

DEVIKA SANTHOSH (180021035904)

DONA JOSE (180021035906)

ELJA GEORGE (180021035909)

VINAYAK KANNAN (180021035939)

PLACE: MUVATTUPUZHA

DATE:

ACKNOWLEDGEMENT

First of all, our gratitude is to **GOD** who showered his divine providence and grace on in the completion this work.

We express our deep sense of gratitude to **Dr. K.V Thomas**, Principal, **Mr. Saji Joseph**, Head of the Department of Mathematics and all staff members of the department for their able and experienced guidance provided invaluably during the period of our study.

We are also grateful to our guide and project coordinator, **Mr. Arun George**, Guest Lecturer on contract, Department of Mathematics, Nirmala College, Muvattupuzha for inducing interest, giving constant encouragement, inspiration and valuable guidance at each and every stage of our project work.

We also thank our family members and friends who were always there with us when we needed them the most.

DEVIKA SANTHOSH

DONA JOSE

ELJA GEORGE

VINAYAK KANNAN

CONTENTS

INTRODUCTION

Today amateurs and professional mathematicians alike know about Diophantine equations and even about Diophantine Analysis. The word Diophantine is derived from the Greek mathematician Diophantus. Diophantus's 'Arithmetica' is the most influential works in the history of mathematics giving numerical solutions to problems. His problems exercised the minds of many of the world's best mathematicians for much of the next to Millennia.

Diophantus's work on equations was continued by Chinese Mathematicians (third century), Arabs (eight through twelfth centuries) and taken to a deeper level by Fermat, Euler, Lagrange, Gauss and many others. This topic remains of great importance in contemporary mathematics.

CHAPTER 1 :
DIOPHANTUS AND DIOPHANTINE EQUATIONS

1.1 DIOPHANTUS

The name 'Diophantine equation' honours the Greek mathematician Diophantus who lived in the third century AD and was one of the first to make a study of equations having integral solutions or in some cases rational solutions.

Most of what is known about Diophantus's life comes from an algebraic riddle from around the early sixth century.

The riddle states:
"Diophantus's boyhood lasted 1/6 of his life. He grew a beard after 1/12 more of his life. After 1/7 more of his life, Diophantus married. Five years later, he had a son. The son lived exactly half as long as his father, and Diophantus died just four years after his son's death".

All of this totals the years Diophantus lived.

What is the age of Diophantus?

If x was the age at which Diophantus died, these data lead to the equation.

$$\frac{1}{6}x + \frac{1}{12}x + \frac{1}{7}x + 5 + \frac{1}{2}x + 4 = x$$

and the solution is x = 84. Thus, he must have reached an age of 84. But in what year or even in what century is not certain.

The great work upon which the reputation of Diophantus rests is his 'Arithmetica', it is the earliest known book on Algebra. Special symbols are introduced to represent frequently occurring concepts, such as the unknown quantity in an equation and the different powers of the unknown up to the sixth power; Diophantus also had a symbol to express subtraction and another for equality. He was the first person known to use algebraic notation and symbolism. Before him everyone wrote out equations completely.

The part of the Arithmetica that has come down to us consists of some 200 problems. Solutions for the equations were usually given in terms of positive rational numbers, sometimes admitting positive integers; there was no notion at

that time of negative numbers as mathematical entities. Of the original thirteen books of which Arithmetica consisted, only six have survived.

Arithmetica inspired some of the world's greatest mathematicians including Euler and Pierre de Fermat to make significant new discoveries. Diophantus is often called "the father of algebra" because he contributed greatly to number theory. The Arithmetica became a treasure trove for number theorists and it remains a source of inspiration to number theorists.

A Diophantine Equation is and algebraic equation usually in two or more unknowns. The coefficient of Diophantine Equation should be integers (rationals; by eliminating the denominators of rational numbers we get an equivalent equation with integer coefficients.).

1.2 Diophantine Equations

A Diophantine Equation is of the form,

$f(x_1,x_2, ... x_n) = 0$

whose coefficients are integers. If this equation has a solution in integers, then $(x_1,x_2, ... x_n)$ is an integral solution.

$2x+3y=4$, $x^2+y^2=1$, $x^2+y^2=z^2$ are examples of Diophantine Equations.

The simplest type of a Diophantine Equation that we shall consider is the Linear Diophantine Equation, in two unknowns.

It is of the form,

$$ax+by=c$$

where a,b,c are given integers and a,b are not both zero.

There is no universal method for determining whether a Diophantine Equation has a solution or for finding them all if solutions exist. A Diophantine Equation may have no solution, a finite number of solutions or an infinite number of solutions.

For example,

The solutions of Diophantine Equation $x^2+y^2=z^2$ represent the lengths of sides of a right angled triangle. (3,4,5) is a solution and thus equation has infinite number of solutions.

The Linear Diophantine equation ax+by = c has a solution if and only if d | c, where d = gcd(a,b) or c is a multiple of d.

Euclidean Algorithm is an efficient method for computing greatest common divisor of two integers which involves repeated application of division algorithm.

Let a and b be two integers. Because gcd (|a|,|b|) = gcd (a,b) there is no harm in assuming that $a \geq b > 0$. Applying Division Algorithm, we get

$$a = q_1 b + r_1 \qquad 0 \leq r_1 < b$$

if $r_1 = 0$, then b|a and gcd (a, b) = b.

if $r \neq 0$ divide b by r_1 we get

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

If $r_2 = 0$ we stop, otherwise the process continue until some zero remainder appears.

The result is the following system of equations

$$a = q_1 b + r_1 \quad 0 \leq r_1 < b$$

$$b = q_2 r_1 + r_2 \quad 0 \leq r_2 < r_1$$

$$r_1 = q_3 r_2 + r_3 \quad 0 \leq r_3 < r_2$$

.

.

.

$$r_{n-1} = q_{n+1} r_n + 0$$

r_n is the last non-zero remainder and gcd(a, b) = r_n

Problem 1

Consider the linear Diophantine Equation,

172x+20y=1000

Applying Euclidean Algorithm to the evaluation of gcd(172, 20) we find that

$$172 = 8*20+12$$

$$20 = 1*12+8$$

$$12 = 1*8+4$$

$$8 = 2*4+0$$

gcd(172, 20) = 4

4 divides 1000. Therefore a solution to this equation exist.

Problem 2

Show that the Diophantine Equation has no solution

$$3x+6y = 2$$

gcd(3,6) = 3

2 is not a multiple of 3

There is no solution for x, y in integers.

Diophantus considered negative or irrational square root solutions useless. It is interesting to note that Diophantus did not restrict his solutions to the integers but recognised rational number solutions as well. Today however the solutions for a so called Diophantine Equations must be integers. The mathematical study of Diophantine problems that Diophantus initiated is now called Diophantine Analysis.

CHAPTER 2 :

SOME CLASSICAL DIOPHANTINE EQUATIONS

2.1 LINEAR DIOPHANTINE EQUATIONS

An equation of the form

$a_1x_1+a_2x_2 \cdots + a_nx_n = c$ …. (1)

where $a_1, a_2, \ldots, a_n$, b are fixed integers, is called a linear Diophantine equation. We assume that $n \geq 1$ and that coefficients $a_n, \ldots, a_n$ are all different from zero

The main result concerning linear Diophantine equations is the following.

Theorem 2.1.1.

Let a, b, c be integers, a and b nonzero. Consider the linear Diophantine equation

$ax + by = c$ ……. (2)

1.The equation (2) is solvable in integers if and only if d = gcd(a, b) divides c.
2. If $(x, y) = (x_0, y_0)$ is a particular solution to equation (2), then every integer solution is of the form

$x = x_0 + \frac{b}{d}t$, $y = y_0 - \frac{a}{d}t$ ……(3) , where t is an integer.

3. If c = gcd(a, b) and |a| or |b| is different from 1, then a particular solution

$(x, y) = (x_0, y_0)$ to equation (3) can be found such that $|x_0| < |b|$ and $|y_0| < |a|$.

Proof

1. If d does not divide c, then the equation is clearly not solvable. If d divides c, then, dividing both sides of equation (2) by $\frac{d}{c}$, it suffices to prove that d is a linear combination with integer coefficients of a and b. For this we use the Euclidean algorithm. Suppose a = bq + r for integers a, b, r, and q. It is easy to see that every common divisor of a and b is a common divisor of b and r, and conversely. Clearly, if b | a, then gcd(a, b) = b. In general, we have gcd(a, b) = gcd(b, r). These observations lead to a straightforward calculation of the gcd of two numbers. To be systematic, we write a = r−1 and b = r_0 (assumed positive and a ≥ b):

$r_{-1} = r_0q_0 + r_1$, $0 \leq r_1 < r_0$,
$r_0 = r_1q_1 + r_2$, $0 \leq r_2 < r_1$,
$r_1 = r_2q_2 + r_3$, $0 \leq r_3 < r_2$,
…….
……

This division process eventually terminates, since the remainders get smaller and smaller, $r_{-1} > r_0 > r_1 > r_2 > \cdots$, and yet remain nonnegative. In other words, some r_n divides the preceding r_{n-1} (and leaves a remainder $r_{n+1}= 0$). We obtain ,

$r_{n-2}= r_{n-1}q_{n-1} + r_n, \qquad 0 \le r_n < r_{n-1},$
$r_{n-1} = r_nq_n$

From these, $r_n= \gcd(r_{n-1}, r_n) = \gcd(r_{n-2}, r_{n-1}) =\cdots= \gcd(r_{-1}, r_0) = \gcd(a, b)$. The above calculation of gcd(a, b) can be retraced to give gcd(a, b) as an integer combination of a and b.

Define the integers x_k and y_k recursively by

$x_k = x_{k-2} - q_{k-1}x_{k-1}, \ x{-}1 = 1, x_0 = 0,$
$y_k = y_{k-2} - q_{k-1}x_{k-1}, \ y{-}1 = 0, y_0 = 1.$

In each of these steps, $r_k = ax_k + by_k$. In particular, $\gcd(a, b) = r_n = ax_n + by_n$. It can be checked that (x_i) and (y_i) alternate in sign, $|x_{n+1}| = b/ \gcd(a, b)$, and $|y_{n+1}| = a/ \gcd(a, b)$. It follows that $|x_n| < b$ and $|y_n| < a$ unless $n = 0$ and $q_0 = 1$, that is, unless $a = b = 1$.

2. We have $ax + by = a [x_0 + \frac{b}{d} t] + b[y_0 - \frac{a}{d}t]= ax_0 + by_0 = c.$
3. The result has already been proven in part 1

Theorem 2.1.2.

The equation (1) is solvable if and only if $\gcd(a_1,...,an) \mid c$.

Proof.

Let $d = \gcd(a_1,...,a_n)$. If c is not divisible by d, then equation (1) is not solvable, since for any integers $x_1,...,x_n$, the left-hand side of equation (1) is divisible by d and the right-hand side is not. Actually, we need to prove that $\gcd(x_1, x_2,...,x_n)$ is a linear combination with integer coefficients of $x_1, x_2,...,x_n$. For $n = 2$ this follows from Theorem 2.1.1. Because $\gcd(x_1,...,x_n) = \gcd(\gcd(x_1,...,x_{n-1}), x_n)$, $\gcd(x_1,...,x_n)$ is a linear combination of x_n and $\gcd(x_1,...,x_{n-1})$. Then inductively $\gcd(x_1,...,x_n)$ is a linear combination of $x_1,...,x_{n-1}, x_n$.

Example 1. Solve the equation $3x + 4y + 5z = 6$.

Working modulo 5,

we have $3x + 4y \equiv 1 \pmod 5$, and hence $3x + 4y =1+5s, s \in Z$.

A solution to this equation is

$x = -1+3s$ $y = 1 - s.$

Applying equation (3), we obtain $x = -1+3s + 4t$, $y = 1 - s - 3t$, $t \in Z$, and substituting back into the original equation yields $z = 1 - s$.

Hence all solutions are

$(x, y, z) = (-1+3s + 4t, 1 - s - 3t, 1 - s)$, $s, t \in Z$.

For any positive integers $a_1,...,a_n$ with $\gcd(a_1,...,a_n) = 1$, define $g(a_1,...,a_n)$ to be the greatest positive integer N for which the equation

$a_1x_1 + \cdots + a_nx_n = N$

is not solvable in nonnegative integers. The problem of determining $g(a_1,...,a_n)$ is known as the Frobenius coin problem.

2.2 PYTHAGOREAN TRIPLES AND RELATED PROBLEMS

One of the most celebrated Diophantine equations is the Pythagorean equation

$X^2 + Y^2 = Z^2$ …….(4)

Studied in detail by Pythagoras in connection with the right triangles whose side lengths are all integers, this equation was known even to the ancient Babylonians. Note first that if the triple of integers (x_0,y_0,z_0) satisfies equation (4), then all triples of the form (kx_0, ky_0, kz_0), $k \in Z$, also satisfy equation (4). That is why it is sufficient to find solutions (x, y, z) to equation (4) with $\gcd(x, y, z) = 1$. This is equivalent to the fact that x, y, z are pairwise relatively prime.

A solution (x_0, y_0, z_0) to equation (4) with x_0, y_0, z_0 pairwise relatively prime is called a primitive solution. It is clear that in a primitive solution exactly one of x_0 and y_0 is even.

Theorem 2.2.1.

Any primitive solution (x, y, z) in positive integers to the equation (4) with y even is of the form

$x = m^2 - n^2$ $y = 2mn$ $z = m^2 + n^2$ (5)

where m and n are relatively prime positive integers such that m>n and m + n is odd.

Proof.

The integers x and y cannot both be odd, for otherwise $z^2 = x^2 + y^2 \equiv 2 \pmod 4$,

a contradiction.

Hence exactly one of the integers x and y is even.

The identity $(m^2 – n^2)^2 + (2mn)^2 = (m^2 + n^2)^2$ shows that the triple given by equation (5) is indeed a solution to the equation (4) and y is even.

Because x must be odd, we may assume without loss of generality that m is odd and n is even. Moreover, if gcd $(m^2 – n^2, 2mn, m^2 + n^2) = d \geq 2$, then d divides

$$2m^2 = (m^2+ n^2)+(m^2 – n^2)$$

and d divides

$$2n^2= (m^2 + n^2)– (m^2 – n^2) .$$

Because m and n are relatively prime it follows that d = 2. Hence $(m^2 + n^2)$ is even, in contradiction to m odd and n even. It follows that d = 1, so the solution equation (5) is primitive.

Conversely, let (x, y, z) be a primitive solution to equation (4) with y = 2a. Then x and z are odd, and consequently the integers z + x and z − x are even.

Let z + x = 2b and z − x = 2c. We may assume that b and c are relatively prime, for otherwise z and x would have a nontrivial common divisor. On the other hand,

$$4a^2= y^2 = z^2 –x^2 = (z + x)(z − x)=4bc,$$

i.e., $a^2 = bc$. Since b and c are relatively prime, it follows that $b = m^2$ and $c = n^2$ for some positive integers m and n. We obtain that m + n is odd and

$$x = b − c = m^2 – n^2, y = 2mn, z = b + c = m^2 + n^2.$$

A triple (x, y, z) of the form equation (5) is called primitive. In order to list all primitive solutions to equation (4), we assign values 2, 3, 4,... to m and then for each of these values we take those integers n that are relatively prime to m and less than m.

Corollary 2.2.2.

The general integral solution to equation (4) is given by

$x = k(m^2 - n^2)$, $y = 2kmn$, $z = k(m^2 + n^2)$, …… (6)

where k, m, n ∈ Z.

The immediate extension to equation (4) is

$$x^2 + y^2 + z^2 = t^2 \text{……. (7)}$$

The positive solutions (x, y, z, t) to equation (7) represent the dimensions and the length of the diagonal of a rectangular box. We want to find all situations in which these components are all integers.

Theorem 2.2.3.

All the solutions to equation (7) in positive integers x, y, z, t with y, z even are given by

$X = \frac{l^2+m^2-n^2}{n}$, $y = 2l$, $z = 2m$, $t = \frac{l^2+m^2+n^2}{n}$…..(8)

where l,m are arbitrary positive integers and n is any divisor of $l^2 + m^2$ less than $\sqrt{(l^2 + m^2)}$. Every solution is obtained exactly once in this way.

Remarks.

A well-known way to produce "Pythagorean quadruples" is

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

where l, m, n are positive integers. It is also known that not all quadruples are generated in this way.

Example

Find all quadruples (x, y, z, w) such that $x^2 + y^2 + z^2 + xy + yz + zx = 2w^2$.

Write the equation as $(x + y)^2 + (y + z)^2 + (z + x)^2 = (2w)^2$.

From Theorem 2.2.3,

$x + y = \frac{l^2+m^2-n^2}{n}$, $y + z = 2l$, $z + x = 2m$, $2w = \frac{l^2+m^2+n^2}{n}$,

where n divides $l^2 + m^2$. It follows that all desired quadruples are

$x = m - l + \frac{l^2+m^2-n^2}{2n}$, $y = l - m + \frac{l^2+m^2-n^2}{2n}$, $z = l + m - \frac{l^2+m^2-n^2}{2n}$, $w = \frac{l^2+m^2-n^2}{2n}$,

where the positive integers l, m, n are chosen such that x, y, z are all positive and 2n divides $l^2 + m^2 + n^2$.

2.3 PELL'S EQUATION

A special case of the quadratic Diophantine equation having the form,
$x^2 - Dy^2 = 1$, where $D>0$
is a non square natural number. In cartesian coordinates the equation has the form of a hyperbola. In 1657, Fermat stated without proof that if D is positive and not the square of an integer, then it has an infinite number of solutions. These solutions may be used to accurately approximate the square root of n by rational numbers.

The equation $x^2 - Dy^2 = -1$ is called negative Pell's equation. It is solvable only for certain values of D.

2.4 FERMAT'S EQUATION

The fermat equation is the Diophantine equation, $x^n + y^n = z^n$, where x, y, z are integers and n is a positive integer greater than 2. Anon trivial solution to the Fermat equation $x^n + y^n = z^n$ is a solution in integers x, y, z where none of x, y, z are zero.

CHAPTER 3:

METHODS FOR SOLVING DIOPHANTINE EQUATIONS

3.1 Solving using Euclidean Algorithm

If $gcd(a,b) \nmid c$, then the linear Diophantine equation ax + by = c has no solution.

If gcd(a,b) | c, then the linear Diophantine equation ax + by = c has a solution.

To solve ax + by =c:

1. Use the Division Algorithm to find d=gcd(a,b).

2. Use the Euclidean Algorithm to find x* and y* such that d = ax* + by*.

3. Find p such that c= dp. (p exists since d | c.)

4. Then x_0 = x*p and y_o = y*p are solutions since c=dp = a(x*p) + b(y*p).

If the linear Diophantine equation ax + by = c does have a solution, then all such solutions are given by

$x = x_o + (b/d)t$ and $y = y_o - (a/d)t$

where d =gcd(a,b), x_o , y_o is a particular solution to the equation and t ranges over the integers.

Example

Find all the positive solutions to the Diophantine equation 172x + 20y = 1000.

- Use the Division Algorithm to find d = gcd(172, 20).

172 = (20*8) +12 ------(1)

20 = (1*12) +8 ------(2)

12 = (1*8) +4 -------(3)

8 = (2*4) +0 ------(4)

gcd= last non-zero remainder=4

- Use the Euclidean Algorithm to find x* and y* such that d = ax* + by*.

from (3) … 4= 12-(1*8)

from (2)…. 4 =12-(1*(20-(1*12)))

= 12-(20-12) = (2*12)-20

from (1)…. 4=2*(172-(20*8))-20

=(2*172)-(20*16)-20

=(2*172)+(-17*20)

$x^* = 2$ and $y^* = -17$

• Find p such that c = dp.

$d = \gcd(172,20) = 4$

$c = 1000$

Therefore, $p = 1000/4 = 250$.

$x_o = x^*p$ and $y_o = y^*p$ are particular solutions

since, $c = dp = a(x^*p) + b(y^*p)$.

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

$1000 = 172*(500) + 20*(-\ 4250)$

So a 'particular' solution is $x_o = 500$ and $y_0 = -\ 4250$.

All solutions are ,

$x = x_o + (b/d)t$ and

$y = y_o - (a/d)t$, where t is an integer.

we know $a = 172$, $b = 20$, $d = 4$, $x_o = 500$ and $y_o = -\ 4250$

So the solutions, in integers, are $x = 500 + 5t$ and $y = -\ 4250 - 43t$ where t ranges over the integers.

To find all the positive solutions we need to find those values of t for which

$x = 500 + 5t > 0$ and $y = -\ 4250 - 43t > 0$.

$x = 500 + 5t > 0$ gives $t > -\ 100$.

$y = -\ 4250 - 43t > 0$

gives $t < -\ 98.83...$ Since t must be an integer, $t \leq -\ 99$.

So $-\ 100 < t \leq -\ 99$.

So there is only one positive solution to the Diophantine equation, namely

$x = 500 + 5t = 5$ and

$y = -\ 4250 - 43t = 7$

3.2 Fermat's Method of Infinite Descent (FMID)

Pierre de Fermat had an enormous impact on the world of mathematics through his discoveries and methods. He was one of the first mathematicians to use a method of proof called the "infinite descent."

Let P be a property concerning the nonnegative integers and let

$(P(n))_{n\geq 1}$ be the sequence of propositions,

P (n): "n satisfies property P ."

The following method is useful in proving that proposition P (n) is false for all large enough n.

Let k be a non-negative integer. Suppose that:

• P (k) is not true;

• whenever P (m) is true for a positive integer $m > k$, then there must be some smaller j, $m > j \geq k$, for which P (j) is true.

Then P (n) is false for all $n \geq k$.

This is just the contrapositive of strong induction, applied to the negation of proposition P (n).

The method described above is often called the finite descent method.

Fermat's method of infinite descent (FMID) can be formulated as follows:

Let k be a non-negative integer. Suppose that:

• whenever P (m) is true for an integer $m > k$, then there must be some smaller integer j, $m > j > k$, for which P (j) is true.

Then P (n) is false for all $n > k$.

That is, if there were an n for which P (n) was true, one could construct a sequence $n > n_1 > n_2 > \cdots$ all of which would be greater than k but for the non-negative integers, no such infinite descending sequence exists.

Two special cases of FMID are particularly useful in the study of Diophantine equations.

FMID Variant 1: There is no sequence of non-negative integers

$n_1 > n_2 > \cdots$

In some situations it is convenient to replace FMID Variant 1 by the following equivalent form: If n_0 is the smallest positive integer n for which P (n) is true, then P (n) is false for all $n < n_0$.

FMID Variant 2: If the sequence of non-negative integers $(n_i)_{i\geq 1}$

satisfies the inequalities $n_1 \geq n_2 \geq \cdots$, then there exists i_0 such that

$n_{i0} = n_{i0+1} = \cdots$.

Example 1

Solve in non-negative integers the equation

$$x^3 + 2y^3 = 4z^3.$$

Solution.

(0, 0, 0) is a solution. We will prove that there are no other solutions. Assume that (x_1 , y_1 , z_1) is a non-trivial solution.

$$x_1 > 0, y_1 > 0, z_1 > 0.$$

From , $x_1^3 + 2y_1^3 = 4z_1^3$ it follows that

$2 \mid x_1$, so $x_1 = 2x_2$, $x_2 \in Z^+$.

Then , $4x_2^3 + y_1^3 = 2z_1^3$ and hence $y_1 = 2y_2$, $y_2 \in Z^+$.

Similarly, $z_1 = 2z_2$, $z_2 \in Z^+$.

We obtain the "new" solution (x_2 , y_2 , z_2) with $x_1 > x_2$, $y_1 > y_2$, $z_1 > z_2$. Continuing this procedure, we construct a sequence of positive integral solutions $(x_n , y_n , z_n)_{n\geq 1}$ such that $x_1 > x_2 > x_3 > \cdots$. But this contradicts FMID Variant 1.

Example 2. Solve in non-negative integers the equation

$$2^x - 1 = xy.$$

Solution.

Note the solutions (0, k), k ϵ Z + , and (1, 1). We will prove that there are no other solutions by using FMID on the prime factors of x. Let p_1 be a prime divisor of x and let q be the least positive integer such that $p_1 \mid 2^q - 1$.

From Fermat's Little Theorem

we have $p_1 \mid 2^{p1-1} - 1$, and therefore $q \leq p_1 - 1 < p_1$.

Let us prove now that q | x. If it didn't, then x = kq + r, with 0 < r < q, and

$$\begin{aligned} 2^x - 1 &= 2^{kq} 2^r - 1 \\ &= (2^q)^k \cdot 2^r - 1 \\ &= (2^q - 1 + 1)^k \cdot 2^r - 1 \\ &\equiv 2^r - 1 \pmod{p_1}. \end{aligned}$$

It follows that $p_1 \mid 2^r - 1$, which contradicts the minimality of q.

Thus q | x and $1 < q < p_1$. Now let p_2 be a prime divisor of q. It is clear that p_2 is a divisor of x and $p_2 < p_1$. Continuing this procedure, we construct an infinite decreasing sequence of prime divisors of x: $p_1 > p_2 > \cdots$, in contradiction to FMID Variant 1.

3.3 The Method of Mathematical Induction

Mathematical induction is a powerful and elegant method for proving statements depending on non-negative integers.

Let $(P(n))_{n \geq 0}$ be a sequence of propositions. The method of mathematical induction assists us in proving that P (n) is true for all $n \geq n_0$, where n_0 is a given non-negative integer.

Mathematical Induction (weak form): Suppose that:

• P (n_0) is true;

• For all $k \geq n_0$, P (k) is true implies P (k + 1) is true.

Then P (n) is true for all $n \geq n_0$.

Mathematical Induction (with steps): Let 's' be a fixed positive integer. Suppose that:

• P (n_0), P ($n_0 + 1$), . . . , P ($n_0 + s - 1$) are true;

• For all $k \geq n_0$, P (k) is true implies P (k + s) is true.

Then P (n) is true for all $n \geq n_0$.

Mathematical Induction (strong form): Suppose that

• $P(n_0)$ is true;

• For all $k \geq n_0$, $P(m)$ is true for all m with $n_0 \leq m \leq k$ implies

$P(k+1)$ is true.

Then $P(n)$ is true for all $n \geq n_0$.

The following examples are meant to show how mathematical induction works in studying Diophantine equations.

Example 1

Prove that the equation $x^2 + (x+1)^2 = y^2$ has infinitely many solutions in positive integers x, y.

Solution.

Note that $x_1 = 3$, $y_1 = 5$ is a solution.

Define the sequences $(x_n)_{n\geq 1}$, $(y_n)_{n\geq 1}$ by,

$$\begin{cases} x_{n+1} = 3x_n + 2y_n + 1 \\ y_{n+1} = 4x_n + 3y_n + 2, \text{ where } x_1 = 3 \text{ and } y_1 = 5. \end{cases}$$

Suppose that (x_n, y_n) is a solution to the equation. Then

$x_{n+1}^2 + (x_{n+1} + 1)^2 = (3x_n + 2y_n + 1)^2 + (3x_n + 2y_n + 2) = (4x_n + 3y_n + 2)^2$

since $x_n^2 + (x_{n+1})^2 = y_n^2$.

Therefore $x_{n+1}^2 + (x_{n+1} + 1)^2 = y_{n+1}^2$

(x_{n+1}, y_{n+1}) is also a solution.

Example 2

Prove that for all positive integers n, the following equation is solvable in integers:

$x^2 + xy + y^2 = 7^n$.

Solution.

If $n = 1$, we have the solution $x_1 = 2$, $y_1 = 1$.

Suppose that there exist positive integers x_n, y_n satisfying

$$x_n^2 + x_n y_n + y_n^2 = 7^n$$

and define

$x_{n+1} = 2x_n - y_n$, $y_{n+1} = x_n + 3y_n$. Hence

$x_{n+1}^2 + x_{n+1} y_{n+1} + y_{n+1}^2 = 7(x_n^2 + x_n y_n + y_n^2) = 7 \cdot 7^n = 7^{n+1}$

3.4 The Modular Arithmetic Method

In many situations, simple modular arithmetic considerations are employed in proving that certain Diophantine equations are not solvable or in reducing the range of their possible solutions.

Example 1

Show that the equation

$(x + 1)^2 + (x + 2)^2 + \cdots + (x + 99)^2 = y^z$

is not solvable in integers x, y, z, with $z > 1$.

Solution.

We notice that

$y^z = (x + 1)^2 + (x + 2)^2 + \cdots + (x + 99)^2$

$= 99x^2 + 2(1 + 2 + \cdots + 99)x + (1^2 + 2^2 + \cdots + 99^2)$

$= 99x^2 + \frac{(2*99*100)}{2} x + \frac{(199*99*100)}{6}$

$=33(3x^2+300x+50*199)$

which implies that $3 \mid y$.

Since $z \geq 2$, $3^2 \mid y^z$,

but 3^2 does not divide $33(3x^2 + 300x + 50*199)$, a contradiction.

Example 2

Find all pairs of positive integers (x, y) for which $x^2 - y! = 2001$

Solution.

For y greater than 5, y! is divisible by 9, so y! + 2001 gives the residue

3 (mod 9), which is not a quadratic residue.

Hence the only candidates are y = 1, 2, 3, 4, 5. Only y = 4 passes, giving

x = 45.

Example 3

Find all pairs of positive integers (x, y) satisfying the equation

$3^x - 2^y = 7$.

Solution.

Let us assume that $y \geq 3$. Reducing modulo 8, we deduce that 3^x must give the residue 7. However, 3^x can be congruent only to 3 or 1 (mod 8), depending on the parity of x. We are left with the cases y = 1 and y = 2, which are immediate. The only solution is x = 2, y = 1.

Example 4.

Determine all primes p for which the system of equations

$$\begin{cases} p + 1 = 2x^2 \\ p^2 + 1 = 2y^2 \end{cases}$$

has a solution in integers x, y.

Solution.

The only such prime is p = 7. Assume without loss of generality that $x, y \geq 0$.

Note that $p + 1 = 2x^2$ is even, so p not equal to 2.

Also,

$2x^2 \equiv 1 \equiv 2y^2 \pmod{p}$, which implies

$x \equiv \pm y \pmod{p}$, since p is odd.

Since $x < y < p$, we have $x + y = p$. Then

$p^2 + 1 = 2(p - x)^2 = 2p^2 - 4px + p + 1$,

so, $p = 4x - 1$, $2x^2 = 4x$, x is 0 or 2, and p is −1 or 7.

−1 is not prime, but for p = 7, (x, y) = (2, 5) is a solution.

3.5 The Factoring Method

Given the equation $f(x_1, x_2, \ldots, x_n) = 0$, we write it in the equivalent form

$f_1(x_1, x_2, \ldots, x_n) f_2(x_1, x_2, \ldots, x_n) \cdots f_k(x_1, x_2, \ldots, x_n) = a$,

where $f_1, f_2, \ldots, f_k \in Z[X_1, X_2, \ldots, X_n]$ and $a \in Z$. Given the prime factorization of a, we obtain finitely many decompositions into k integer factors $a_1, a_2, \ldots, a_k$. Each such factorization yields a system of equations

$$\begin{cases} f_1(x_1, x_2, \ldots, x_n) = a_1 \\ f_2(x_1, x_2, \ldots, x_n) = a_2 \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ f_k(x_1, x_2, \ldots, x_n) = a_k \end{cases}$$

Solving all such systems gives the complete set of solutions

Example 1

Solve the following equation in integers x, y:

$x^2 + 6xy + 8y^2 + 3x + 6y = 2$.

Solution.

Write the equation in the form

$$(x + 2y)(x + 4y) + 3(x + 2y) = 2$$

ie $$(x + 2y)(x + 4y + 3) = 2.$$

the possibilities are

$$\begin{cases} x+2y=2 \\ x+4y+3=1 \end{cases}$$

$$\begin{cases} x+2y=1 \\ x+4y+3=2 \end{cases}$$

$$\begin{cases} x+2y=-2 \\ x+4y+3=-1 \end{cases}$$

$$\begin{cases} x+2y=-1 \\ x+4y+3=-2 \end{cases}$$

solving these 4 pairs of equations we obtain the solutions

$(0, -1), (3, -2), (3, -1), (6, -2)$.

Example 2

Solve the Diophantine equation $x - y^4 = 4$, where x is a prime.

Solution.

The equation is equivalent to $x = (y^2 + 2)^2 - (2y)^2$

$x = [(y-1)^2 + 1][(y+1)^2 + 1]$

If y not equal to ± 1, x is a product of two integers greater than 1; hence it

is not a prime. The solutions are (5, 1), (5, −1).

3.6 Solving Diophantine Equations Using Inequalities

This method consists in restricting the intervals in which the variables lie using appropriate inequalities. Generally, this process leads to only finitely many possibilities for all variables or for some of them.

Example 1

Determine all triples of positive integers (x, y, z) that are solutions to the equation

$(x + y)^2 + 3x + y + 1 = z^2$.

Solution.

The inequalities $(x + y)^2 < (x + y)^2 + 3x + y + 1 < (x + y + 2)^2$

imply $(x + y)^2 + 3x + y + 1 = (x + y + 1)^2$.

It follows that $x = y = k \in Z^+$;

hence all the solutions are (k, k, 2k + 1).

Example 2

Determine all pairs of integers (x, y) that satisfy the equation

$(x + 1)^4 - (x - 1)^4 = y^3$

Solution.

We have $(x + 1)^4 - (x - 1)^4 = 8x^3 + 8x$.

Suppose a pair (x, y) of integers is a solution and assume $x \geq 1$. Then

$$(2x)^3 < (x+1)^4 - (x-1)^4 < (2x+1)^3 .$$

Hence $2x < y < 2x+1$, a contradiction.

Therefore, for every solution (x, y), the integer x must be non-positive. Now observe that if (x, y) is a solution, then (−x, −y) is also a solution; hence −x must be non-positive. Therefore (0, 0) is the only solution.

Chapter 4

Applications of Diophantine Equations

4.1 Pythagorean Theroem

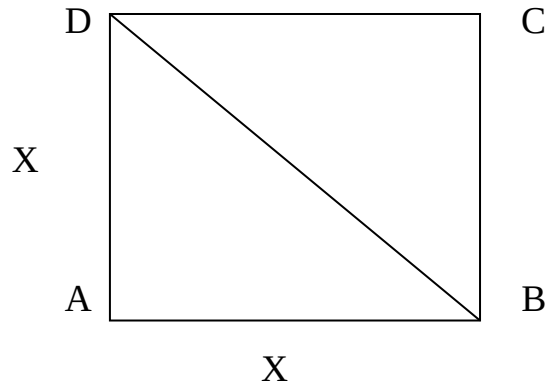
The Pythagorean theorem is based on a set of Diophantine equations of degree two of the form $x^2+y^2=z^2$.In this form of equation x^2 ,y^2 and z^2 can each represent a Diophantine equation of degree two, specifically when these Diophantine equations have a numerical value equal to a squared integer.Thus Pythagorean triples are among the oldest known solutions of a nonlinear Diophantine equations.

Example1

Find the area of a square of diagonal 100m

Solution .

A square of side x and diagonal 100 m is shown below,



The Pythagorean theorem is given by $x^2+y^2=z^2$

Here y=x z=100cm

$x^2+y^2=100^2$

$2x^2 = 100^2$

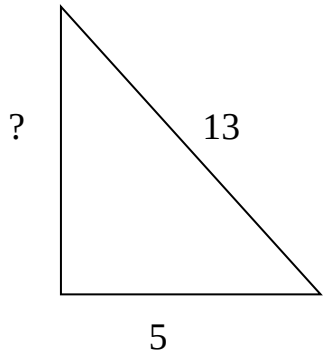
$x^2 = 10000/2$

$=5000$

Area of the square=$x^2=5000m^2$

Example 2

Calculate the height that we can reach with a 13 feet ladder leaning against a wall if the bottom of the ladder is 5 feet from the wall



Let x be the height of the wall we can reach with a ladder of length y,z and y be the distance between foot of the wall and foot of the ladder $x^2+y^2=z^2$

Therefore x $=\sqrt{z^2-y^2}$

$=\sqrt{13^2-5^2}$

$=\sqrt{169-25}$

$=\sqrt{144}$

=12

So the height is 12 feet.

4.2 Hundred Fowls Problem

1)If a cock is worth five coins, a hen 3 coins and 3chicks together one coin . How many cocks' hens and chicks totalling 100 can be bought for 100 coins?

Let x ,y and z denote the number of cocks the number of hens and number of chicks respectively.

Clearly x ,y ,z ≥0.Then the given data yield 2 linear Diophantine equations

x+y+z=100 (strength) →①

5x+3y+z/3=100 (price) →②

Substitute ,

Z =100-x-y in ②

$=5x+3y+\frac{1}{3}[100-x-y] = 100$

ie

7x+4y=100

$$y=\frac{100-7x}{4}$$

$$=25-\frac{7x}{4} \qquad \rightarrow ③$$

So,for y to be an integer,$7\frac{x}{4}$ must be integer but 4 does not divides 7, so x must be a multiple of 4.

Therefore , x= 4t , t =integer

(eqn 3) implies , $y = 25-7\frac{x}{4}$

$$=25-\frac{7(4t)}{4}$$

$$=25-7t$$

And $z=100-x-y$

$$=100-4t-(25-7t)$$

$$=75+3t$$

Therefore thus solutions of the puzzle is of the form

x= 4t y=25-7t z=75+3t

Now to find the possible actual solutions of the puzzle, we take the following steps:

Since $x\geq 0$, $t\geq 0$, since $y \geq 0$; $25-7t\geq 0$,

ie, $t<25/7$ so $t\leq 3$

Since $z\geq 0$, $75+3t\geq 0$, ie $t\geq -25$

But this doesn't give us any additional information

So,$0\leq t\leq 3$

Thus the riddle has 4 solutions,

Corresponding to t= 0,1,2,3

x=0, y=25, z=75

x=4, y=18, z=78

x=8, y=11, z=81

x =12, y=4, z=84

4.3 The Balancing Of Chemical Equations

Another applications of Diophantine Equations is in the field of chemistry. Chemical equations can be balanced with the help of Diophantine Equations. A chemical equation is nothing but a chemical reaction when the left side shows the input ,the right side shows the output from the input.

Example

Consider the chemical equations

$x_1C_7H_6O_2+x_2O_2 \rightarrow X_3CO_2+X_4H_2O$

We have to find out the values of x_1, x_2, x_3 and x_4.Since there are 3 types of atoms, we can form 3 equations

For C, $7x_1=x_3$ $\rightarrow$①

For H, $6x_1=2x_4 \Rightarrow 3x_1=x_4$ $\rightarrow$②

For O, $2x_1+2x_2=2x_3+x_4$ $\rightarrow$③

Substituting equation ①and ②in equation ③we get

$2x_1+2x_2=14x_1+3x_1$

⇨ $2x_2=15x_1$

This is a linear Diophantine Equation in 2 unknowns with solution

$x_1=2$ and $x_2=15$

Hence $x_3=14$ and $x_4=6$

The balanced equations becomes,

$2C_7H_6O_2+15O_2 \rightarrow 14CO_2+6H_2O$

CONCLUSION

Diophantine equations are algebraic equations whose solutions are required to be integer numbers. They have captured the attention of mathematicians during millennia and are at the centre of much contemporary research the goal in solving Diophantine equation is to determine if there any solutions and if there are to find all solutions. A complete solution of equation is possible only for a limited types of equation. Also for equation of degree higher than the second in two or more unknowns, the problem becomes rather complicated. Even the more simple problem of establishing whether the number of integral solution is finite or infinite present extreme difficulties.

A common criticism of Diophantine is that it never developed a general method of solutions to his problems. Most of the Diophantine equations required advanced techniques and tools to solve. Some Diophantine equations are easy, while some others are truly difficult. After sometime spent with these equations it might seem that no matter what powerful methods we learn or develop there will always be a Diophantine equation immune to them, which requires a new trick, a better idea, or a refined technique.

REFERENCES

1: Titu Andreescu Dorin Andrica, Ion Cucurezeanu – An Introduction to Diophantine Equations.

2: Isabella G Bashmakova – Diophantus and Diophantine Equations