Some Interesting Results on Diophantine Equations and Euler's Totient Function

BY

K. Raitha

A DISSERTATION SUBMITTED TO THE AVINASHILINGAM INSTITUTE FOR HOME SCIENCE AND HIGHER EDUCATION FOR WOMEN (DEEMED UNIVERSITY) COIMBATORE-43 IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE DEGREE OF **MASTER OF SCIENCE IN MATHEMATICS**

MAY 1996

SOME INTERESTING RESULTS ON DIOPHANTINE EQUATIONS AND EULER'S TOTIENT FUNCTION

By

K. ANITHA

A DISSERTATION SUBMITTED TO THE

AVINASHILINGAM INSTITUTE FOR HOME SCIENCE

AND HIGHER EDUCATION FOR WOMEN

(DEEMED UNIVERSITY)

COIMBATORE - 641 Ø43

IN PARTIAL FULFILMENT OF THE REQUIREMENTS

FOR THE DEGREE OF

MASTER OF SCIENCE IN MATHEMATICS

MAY - 1996

CERTIFIED AS BONAFIDE RESEARCH WORK

K. N. Meenakshi

SIGNATURE OF THE GUIDE

K. N. Meenakshi

SIGNATURE OF THE
HEAD OF THE DEPARTMENT

9.5.96.

SIGNATURE OF THE
DEAN OF THE FACULTY

Acknowledgement

ACKNOWLEDGEMENT

The author is grateful to **PADMASRI COLONEL Dr. (Tmt.) RAJAMMAL P. DEVADAS, M.A., M.Sc., Ph.D. (Ohio State), D.Sc. (Madras), Hon DHL (Oregon State),** Chancellor, Avinashilingam Institute for Home Science and Higher Education for Women (Deemed University), Coimbatore, for all facilities given to her in the course of dissertation.

She expresses her gratitude to **Dr.(Tmt.) LAKSHMI SANTA RAJAGOPAL, M.S., (Tennessee), Ph.D. (Madras),** Vice Chancellor, Avinashilingam Institute for Home Science and Higher Education for Women(Deemed University), Coimbatore for providing facilities to carry out the study.

The author extends her deep sense of gratitude to **Dr.(Tmt.)SAROJA PRABAKARAN, M.A., Dip. in Ed., (Madras) Ph.D., (Mother Teresa)** Registrar of Avinashilingam Institute for Home Science and Higher Education for Women (Deemed University). Coimbatore, and to **Dr. (Tmt.) NIRMALA K.MURTHY, B.Sc., (Hons) (Annamalai), M.S., (IOWA), Ph.D. (Madras),** Dean, Faculty of Science, Avinashilingam Institute for Home Science and Higher Education for Women (Deemed University). Coimbatore, for the keen interest shown by them.

The author wishes to place on record her indebtedness to **Dr. K.N.MEENAKSHI, M.Sc., Ph.D. (Madras),** Professor and Head of the Department of Mathematics, Avinashilingam Institute for Home Science and Higher Education for Women (Deemed University). Coimbatore, for her constant benovelent help, invaluable advice and illuminating guidance. She gratefully acknowledges her persistent efforts and affectionate endeavours.

The author would like to extend her thanks to other staff members and to her friends who were responsible for the good finish of the dissertation.

The author is greatly indebted to her loving parents and brother for being the motivating forces behind this dissertation and providing moral support in carrying out the work.

Contents

CONTENTS

Introduction

INTRODUCTION

Number theory is considered to be the Queen of all branches of Mathemtics. Some of the celebrated names of Mathematicsans who have done research in Number theory are Srinivasa Ramanujam, P. Fermat, Euclid, Minkowski, Goldbach, P.Bachmann, R.D.Carmichael, Diophantine, Dirichlet, L.E.Dickson, G.H. Hardy, Kronecker, Lagrange and Mersenne.

The aim of this thesis is to discuss a few interesting results from Number theory. These results deal with Diophantine equations, Waring's problem and two interesting extensions of the Euler's totient function.

In the first chapter we shall discuss the following problems

1) Integral solutions of the Diophantine equation ax+by=c.

2) The Diophantine equation $X^2 + Y^2 = Z^2$

3) Expressing every positive integer as a sum of four squares and as a sum of five positive squares

4) Waring's problem

5) Given n to find the number of solutions of the equation $x^2 + y^2 = n$

6) Every integer is a sum or difference of 28 integral eighth powers

7) Solutions of the Diophantine equation
$x^6 + y^6 + z^6 = u^6 + v^6 + w^6$

A integer triple (x,y,h) is said to be Pythagorean if $x^2 + y^2 = h$

There are two interesting papers on pythagorean triples.

The first one entitled "Multiple pythagorean number triples" was published by Albert Fassler [2] in the year 1991.

The second one "on the distribution of pythagorean triangles" by J.Lambek and L.Moser [6] was published in 1955.

These two authors have studied the problem of finding the number of pythagorean triples having.

a) Common Hypotenuse **h**

b) Common Leg - sum **s**

c) Common Leg - difference **d**

d) Common Area **f**

e) Common perimeter **p**

f) Common inradius **i**

g) The distribution of pythagorean triangles

In chapter -2 we discuss two interesting extension of Euler's totient function $\phi(n)$.

In section -1 of chapter -2, we collect some well known results on Euler's totient funtion $\phi(n)$.

In section -2, we discuss the proof of the inequality $\phi(n) \geq \sqrt{n}$ for all natural numbers n except for n=2 and 6.

This inequality was established by A.M Vaidya [8] in 1967.

In section -3 we discuss the extension $\phi_f(n)$ of P.Kesava Menon [5] in 1967.

The fuction $\phi_f(n)$ is defined as follows.

Definition:

Given a polynomial f(x) with integral Co-efficients for each n, $\phi_f(n)$ is defined to be the number of residues x modn for which f(x) is prime to n.

This fuction $\phi_f(n)$ is multiplicative. A product formula for $\phi_f(n)$ is established in the follwing form

$$\phi_f(n) = n \prod_{p/n} (1-f_p/P)$$

Where the product is over all distinct prime factors p of n and f_p denotes the number of distinct roots of the congruence.

$$f(x) \equiv O(\text{mod } P)$$

using this result the author is able to develop many interesting applications.

For example, he has obtained the following theorem

Let S : { m_1, ... m_r} be a given set of numbers and let N(p) be the number of distinct residues modP among them for any prime P. Then the number of sequences.

$$a+m_1,\ a+m_2\ .....\ a+m_r \pmod{n}$$

in which all terms are prime to n is equal to

$$n \prod_{p/n} \{1- N(p)/P\}$$

Some very interesting special cases of this theorem are also discussed

In section -4 we discuss the extension of Euler's ϕ function by Nagesware Rao [7]

Definition:

If K is any integer ≥ 1 and A,B are any two integer not both zero then $(A,B)_K$ denotes the largest common divisor of A and B which is also a K - th power.

Definition :

Given positive integers K and M, $\phi_K(M)$ is the number of non-negative integers x less than M^K such that $(x,M^K)_K = 1$.

The author has established the following product formula

$$\phi_K(M) = M^K(1-1/p_1)^K \ldots\ldots 1 -1/p_t)^K$$

where P_1, P_2....P_t are all distinct prime factors of M. The author is able to generalize many of the well known properties of $\phi(n)$ for his function $\phi_K(M)$.

Review of Literature

REVIEW OF LITERATURE

Number theory is considered to be the Queen of all branches of Mathematics. Some of the celebrated names of Mathematics who have done research in Number theory are Srinivasa Ramanujam, P. Fermat, Euclid, Minkowski, Goldbach, P. Bachmann, R.D.Carmichael, Diophantine, Dirichlet, L.E.Dickson, G.H. Hardy, Kronecker, Lagrange and Mersenne.

Some of the important topics in the study of Number theory are as follows

1) Distribution of ~~time~~ primes
2) Diophantine equations
3) Partition of numbers
4) Study of arithmetic functions $\mu(n)$, $\sigma(n)$, $d(n)$ and $R(n)$
5) The representation of a number as a sum of two, four and five squares.
6) Geometry of Numbers

Since Number theory is an age old branch of Mathematics, the origin of the study of these topics is very difficult to find. A beautiful introduction to the theroy of numbers can be found in the classical work of G.H. Hardy and E.M Wright published in 1938. This book contains an ocean of information on the topics mentioned above.

There are many good works on Number theory. To mention a few we have

1. An introduction to the theory of numbers

by IVAN NIVEN & HERBERT S.ZUCKERMAN

2. Introduction to analytic Number theory

by A.M.APOSTOL

3. A selection of problems in the theory of numbers

by WACLAW SIERPINSKI

4. Ingenuity in Mathematics

by HONSBERGER

5. An Introduction to the theory of numbers

by G.H.HARDY & E.M.WRIGHT

Chapter I

CHAPTER - 1

DIOPHANTINE EQUATIONS

In this Chapter we shall discuss the following problems.

1. Integral solutions of the Diophantine equation $ax + by = c$.

2. The Diophantine equation $X^2 + Y^2 = Z^2$

3. Expressing every positive integer as a sum of four squares and as a sum of five positive squares.

4. Waring's problem

5. Given n to find the number of solutions of the equation $x^2 + y^2 = n$

6. Every integer is a sum or difference of 28 integral eighth powers.

7. Solutions of the Diophantine equation $x^6+y^6+z^6 = u^6+v^6+w^6$.

SECTION - I

STUDY OF THE DIOPHANTINE EQUATIONS ax + by = c.

Here we shall discuss the problem of finding all solutions of the above equation and also the number of positive solutions of this equation.

We shall also discuss some specific examples.

To start with, assume $a \neq 0$ and $b \neq 0$

Let $g = (a,b)$ g can be expressed as $ax_0 + by_0$.

If $g \nmid c$ then the equation $ax + by = c$ cannot have a solution in integers.

If g/c

$$\text{Let } x_1 = \frac{c}{g} x_0 \text{ , } y_1 = \frac{c}{g} y_0 \text{ then } ax_1 + by_1 = c.$$

By a simple argument, we can show that every integral solution r,s of ax+by = c can be written in the form.

$$r = x_1 + \frac{b}{g} t \text{ , } s = y_1 - \frac{a}{g} t$$

Where t is any integer

For example

Consider the equation $3x + 5y = 11$.

Here a=3, b=5, c=1, g=1 and

$3(2) + 5(-1) = 1$

We get $X_0 = 2$ and $Y_0 = -1$

Since g=1, $x_1=2$ and $y_1 = -1$

∴ All solutions of this equation can be written in the form $x = 2+5t$, $y= -1-3t$

These solutions can also be expressed as $x = 2-5t$, $y = -1+3t$

We can get yet another form for these solutions by taking

$x = -3+5t$, $y=2-3t$

To get the number of positive solutions for the equation

$ax+by = c$

Consider the expression

$$r = x_1 + \frac{b}{g} t \ , \ s = y_1 - \frac{a}{g} t$$

If both r and s are to be positive

$$x_1 + \frac{b}{g} t > 0 \text{ and } y_1 - \frac{a}{g} t > 0$$

This gives us the condition

$$-\frac{g}{b} x_1 < t < \frac{g}{a} y_1$$

. . If N is the number of positive solutions

N must lie between

$$-\left[\left[-\frac{g}{a} y_1 - \frac{g}{b} x_1\right] + 1\right] \leq N \leq -\left[-\frac{g}{a} y_1 - \frac{g}{b} x_1\right]$$

Consider the equation $5x+3y = 52$

Here $a=5$, $b=3$, $c=52$ and $g=1$ we get

$x_0 = 2$, $y_0 = -3$ and

$x_1 = 104$, $y_1 = -156$

The positive values are given by taking

$t = -34, -33, \text{ or } -32$

The Corresponding 3 solutions are

1. $r=2$, $s=14$
2. $r=5$, $s=9$
3. $r=8$, $s=4$

If we apply the inequality

$$-\left[\left[-\frac{g}{a}\right]y_1 - \frac{g}{b}x_1\right] + 1 \leq N \leq -\left[-\frac{g}{a}y_1 - \frac{g}{b}x_1\right]$$

for this problem we get $3 \leq N \leq 4$.

SECTION - 2

In this section we shall study the equation $X^2 + Y^2 = Z^2$

The following two theorems are well known.

Theorem : 1.2 .1

The positive primitive solutions of $x^2 + y^2 = z^2$ with y even are $x = r^2 - s^2$, $y = 2rs$, $z = r^2 + s^2$ where r and s are arbitrary integers of opposite parity with $r > s > o$ and $(r,s) = 1$

Using the above result we can easily prove the following result.

Theorem : 1.2.2

The only integral solutions of $x^4 + y^4 = z^2$ are the trivial solutions $x=0$, $y,z = \pm y^2$ and $x,y = 0$, $z = \pm x^2$

The following result is an immediate consequence of the above theorem.

Remark : 1. 2.3

For any positive integer $n \equiv 0 \pmod 4$ the equation $x^n + y^n = z^n$ has no solutions with $xy \neq 0$.

Consider

$$x^{4n} + y^{4n} = z^{4n}$$

$X = x^n$, $Y = y^n$, $Z = z^{2n}$

$\therefore X^4 + Y^4 = Z^2$

Since the only solutions are $x = 0$, $y, z = \pm y^2$ and $x, y = 0$, $z = \pm x^2$

Proof of theorem : 1.2.1

Consider a triple x, y, z such that $x^2 + y^2 = z^2$ such that $(x, y, z) = 1$

Then x and y cannot be both even and cannot be both odd. Assume y is even x and z odd.

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

$$\therefore \left[\frac{z + x}{2}\right] \times \left[\frac{z - x}{2}\right] = \left[\frac{y}{2}\right]^2$$

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

We have used the above theorem to arrive at the following results.

1) $21^2 + 20^2 = 29^2$

   $441 + 400 = 841$

2) $11^2 + 60^2 = 61^2$

   $121 + 3600 = 3721$

3) $33^2 + 56^2 = 65^2$

   $1089 + 3136 = 4225$

4) $5^2 + 12^2 = 13^2$

   $25 + 144 = 169$

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

   $9 + 16 = 25$

6) $7^2 + 24^2 = 25^2$

$49 + 576 = 625$

7) $13^2 + 84^2 = 85^2$

$169 + 7056 = 7225$

8) $15^2 + 112^2 = 113^2$

$225 + 12544 = 12769$

9) $17^2 + 144^2 = 145^2$

$289 + 20736 = 21025$

10) $21^2 + 220^2 = 221^2$

$441 + 48400 = 48841$

There are two interesting papers on pythagorean triples

The first one, entitled **"Multiple pythagorean number triples"** was published by Albert Fassler in the year 1991.

The second one **"on the distribution of pythagorean triangles"** by J.Lambek and L.Moser was published in 1955.

These two authors have studied the problem of finding the number of pythagorean triples having.

a) Common Hypotenuse **h**

b) Common Leg - sum **s**

c) Common Leg - difference **d**

d) Common Area **f**

e) Common perimeter **p**

f) Common inradius **i**

g) The distribution of pythagorean triangles

The main results proved in these papers are as follows.

Theorma 1.2.4

If the number $h > 1$ is of the form

$h = P_1^{\beta_1} P_2^{\beta_2} \ldots\ldots\ldots\ldots P_n^{\beta_n}$ where each P_i is prime and $Pi \equiv i \pmod 4$ and $\beta_i \geq 1$ then there are exactly 2^{n-1} different primitive Pythagorean triples with common hypotenuse h and if h is not of this form then there is no primitive pythagorean triple.

Theorem: 1.2.5

If S is of the form

$P_1^{\beta_1} P_2^{\beta_1} \ldots\ldots P_n^{\beta_n}$

where each P_i is of the form $8m \pm 1$. Then there are exactly 2^{n-1} different primitive Pythagorean triples with common leg sum s.

Theoren 1.2.6

There exists no two non congruent right angled triangles with two of the following items in common, hypotenuse, leg sum, leg-difference, area, perimeter, inradius and one leg.

Let P_h (n) (P_p (n)) denotes the number of primitive pythogorean triangles with hypotenuse h (perimeter p) less than or equal to n.

Then P_h (n) and (P_p (n)) satisfy the following asmptotic formula

$$P_h (n) = 1/2 \quad \Pi^{-1} n + O (n^{1/2} \text{ Logn})$$

$$P_p (n) = \text{Log } 2 \quad \Pi^{-2} n + O (n^{1/2} \text{ Logn})$$

SECTION - 3

The aim of the section is to give a short proof of the following theorem.

Theorem : 1.3.1

Every positive integer is a sum of four squares and fewer than four squares will not suffice in general.

Every sufficiently large positive integer is a sum of five positive squares of integers. This result is false if five is replaced by four.

Lemma : 1.3.2

If x and y can be expressed as a sum of four squares then the product xy can also be expressed as a sum of four perfect squares.

Proof

Proof follows by the following identity

Suppose $X = (x_1^2 + x_2^2 + x_3^2 + x_4^2)$ and

$Y = (y_1^2 + y_2^2 + y_3^2 + y_4^2)$

Then

$$\begin{aligned} XY &= (x_1^2 + x_2^2 + x_3^2 + x_4^2) \times (y_1^2 + y_2^2 + y_3^2 + y_4^2) \\ &= (x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4)^2 \\ &+ (x_1y_1 - x_2y_1 + x_3y_4 - x_4y_3)^2 \\ &+ (x_1y_3 - x_3y_1 + x_4y_2 - x_2y_4)^2 \\ &+ (x_1y_4 - x_4y_1 + x_2y_3 - x_3y_2)^2 \end{aligned}$$

By the above lemma it is enough to consider only odd prime numbers.

Lemma : 1. 3.3

Let p denote any odd prime then there exists an integer m such that $1 \leq m < p$ and

$$mp = x_1^2 + x_2^2 + x_3^2 + x_4^2$$

for some integers x_1, x_2, x_3, x_4

Proof

Let $S_1 = \left\{ 0^2, 1^2, 2^2, 3^2, 4^2 \ldots \left| \frac{P-1}{2} \right|^2 \right\}$

$$S_2 = \left\{ -0^2-1, -1^2-1, -2^2-1, \ldots - \left| \frac{P-1}{2} \right|^2 - 1 \right\}$$

Now no two numbers of S_1 are congruent modulo p, and no two numbers of S_2 are congruent mod P.

S_1 and S_2 together contain (P+1) integers since there are only P-distinct residue classes modP. We see that some number of S_1 must be congruent to some number of S_2 modulo P.

$\therefore$ There exist x and y such that

$$x^2 \equiv - y^2 - 1 \pmod{p}$$

(ie) $x^2 + y^2 + 1 \equiv 0 \pmod{p}$ where $0 \leq x, y \leq \frac{p-1}{2}$

$\therefore x^2 + y^2 + 1 = mp$

It is easily seen that $m = \frac{1}{p}(x^2 + y^2 + 1) < p$

Lemma : 1.3.4

If m is the least integer satisfying lemma 1.3.3 then m = 1.

Proof

It can be easily seen that m cannot be even

Assume m>1 and m is odd

Then by using congruence property we can find n such that $0<n<m$ and

$$np = x_1^2 + x_2^2 + x_3^2 + x_4^2$$

Since m is least, m must be equal to 1.

Proof of the theorem : 1.3.5

The three lemmas show that every positive integer is a sum of four squares. We have only to prove the second part of the theorem.

The integers 1,2,3,4,6,7,9,10,12,15,18 and 33 cannot be expressed as a sum of five positive squares. It can be checked that the rest of the positive numbers upto 169 can be expressed in five squares form. So it is enough to consider $n \geq 170$.

The number n-169 can be written as

$$x^2 + y^2 + z^2 + w^2$$

We can assume $x \geq y \geq z \geq w \geq 0$. If x,y,z, w are all positive then

$$n = 13^2 + x^2 + y^2 + z^2 + w^2$$

If x,y,z are positive but w=0 we can write

$$n=12^2 + 5^2+x^2+y^2+z^2$$

If x and y are positive and z=w=0. We can write

$$n=12^2+4^2+3^2+x^2+y^2.$$

If x is only positive we get $n = 10^2 + 8^2 + 2^2 + 1^2 + x^2$

Thus we have proved that every integer can be expressed as a sum of five positive integer squares.

To complete the proof we have to show that there are infinitely many integers which cannot be expressed as a sum of four positive squares of integers.

First note that an integer 2k is a sum of four positive squares iff 8k is such a sum.

Now observe that 8 is not a sum offour positive squares of integers.

This leads to an infinite chain of integers 8,32,128, 152 ..... $2^{2\ c+1}$ which are not sums of four positive squares.

SECTION - 4

In 1770 Edward waring stated the following problem.

Can every positive integer be expressed as a sum of atmost g(k), k^{th} powers of positive integers where g(k) depends only on k, not on the number being represented?

The case k = 2 had been stated by Fermat in 1640 and was attacked unsuccessfully by Euler for a very long time. It was finally proved by lagrange in 1770, who showed that each positive integer could be expressed as a sum of atmost four squares of positive integers.

During the next 139 years, special cases of the problem were solved for k = 3,4,5,6,7,8,10. It was in 1909 that Hilbert solved the problem in the affirmative for all k. His proof was extremely complicated in its detailed arguments.

It is well known that g(2) = 4 and g(3) = 9 and also it is known that

$19 \leq g(4) \leq 35$ and $37 \leq g(5) \leq 54$

Here we present a simple proof to show that $g(4) \leq 50$.

Consider the identity

$$(x_i + x_j)^4 + (x_i - x_j)^4 = 2x_i^4 + 12 x_i^2 x_j^2 + 2x_j^4$$

summing this identity we get ,

$$\sum_{1\le i<j\le 4} \left[(x_i+x_j)^4 + (x_i-x_j)^4 \right]$$

$$= 2 \sum_{i=1}^{4} (4-i)\, x_i^4 + 6 \sum_{i=1}^{4} \sum_{\substack{j=1 \\ j\neq i}}^{4} x_i^2 x_j^2 + 2 \sum_{j=1}^{4} (j-1)\, x_j^4$$

$$= 2 \sum_{i=1}^{4} (4-i+i-1)\, x_i^4 + 6 \sum_{i=1}^{4} \sum_{\substack{j=1 \\ j\neq i}}^{4} x_i^2 x_j^2$$

$$= 6 \sum_{i=1}^{4} x_i^4 + 6 \sum_{i=1}^{4} \sum_{\substack{j=1 \\ j\neq i}}^{4} x_i^2 x_j^2$$

$$= 6 \sum_{i=1}^{4} \sum_{j=1}^{4} x_i^2 x_j^2$$

$$= 6 \left[\sum_{i=1}^{4} x_i^2 \right]^2$$

$$\therefore \sum_{1\le i<j\le 4} \left[(x_i+x_j)^4 + (x_i-x_j)^4 \right] = 6 \left[\sum_{i=1}^{4} x_i^2 \right]^2$$

In the above equation, left hand side is the sum of 12 fourth powers, right hand side is of the form $6m^2$.

Now consider any number of the form 6L,

L - can be expressed as a sum of four numbers of the form m^2.

$\therefore$ 6L is expressed as a sum of 48 fourth powers.

To complete the proof we observe that the integers $j = 0,1,2,81,16,17$ form a complete residue system mod 6 and each one is the sum of atmost 2 fourth powers.

Now every integer $n>81$ can be expressed in the form $61+j$ where $j = 0,1,2,81,16,17$.

Consider $0<n\leq 50$

$$n = \sum_{i=1}^{n} 1^4$$

For $50 <n\leq 81$

$$n = 2^4 + 2^4 + 2^4 + \sum_{i=1}^{n-48} 1^4$$

Hence every integer >81 can be expressed as a sum of atmost 50 fourth powers.

SECTION - 5

In this section we shall discuss the equation $x^2 + y^2 = n$

The problems under consideration are

1. For which values of n, we can solve $x^2 + y^2 = n$?
2. What can we say about the number of solutions of $x^2+y^2 = n$ for a given n ?

We shall collect some results on these two problems.

Notations:

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 $x^2 + y^2 = n$

Definition 1.5.1

A multiplicative function h(n) is defined by $h(1)=1$, $h(2^e)=0$, $h(p^e)=(-1)^{(p-1/2)e}$

Let h(n) for composite n be determined in such a way that h(n) is a multiplicative function with these notations we have the following results.

Result : 1.5.2

We have $N(1) = Q(1) = 4$, $P(1) = 2$ and for $n>1$, $Q(n) = 4P(n)$

and $$N(n) = \sum_{d^2/n} Q\left[\frac{n}{d^2}\right]$$

Result : 1.5.3

Suppose n>1 Each non-negative primitive solution of x^2+y^2 =n determines a unique 'S' modulo n such that sy ≡ x(modn). Further more, S^2 ≡ -1 (modn) and different non-negative primitive solutions determine different S Modulo n.

Result : 1.5.4

Suppose n>1, S^2 ≡ -1 (Modn). there is a non-negative primitive solution x,y of x^2+y^2 = n such that sy ≡ x (modn)

Result : 1.5.5

The functions R(n) and N(n)/4 are multiplicative functions.

Result : 1.5.6

$$N(n) = 4 \sum_{d/n} h(d)$$

Result : 1.5.7

N(n) is four times the excess of the number of divisors of n of the form 4j+1 over those of the form 4j+3

Result ; 1.5.8

The equation $x^2 + y^2 = n$ is solvable if and only if the canonical factoring of n into prime powers contains no factor P^e with P of the form 4j+3 and e odd.

Now we shall discuss two examples when n has a factor of the form 4j+3

1) Consider n = 56 divisors are 1, 2, 4, 7, 8

$$N(n) = 4 \sum_{d/n} h(d) = 4\ (1 - 1)$$

$$= 0$$

$\therefore$ 56 cannot be expressed as the sum of two perfect squares.

2) Consider n = 7 x 5 x 101

divisors are 1, 5, 7, 35, 101, 505, 707, 3535

$$N(n) = 4 \sum_{d/n} h(d) = 4\ (1 + 1 - 1 - 1 + 1 + 1 - 1 - 1)$$

$$= 0$$

$\therefore$ 7 x 5 x 101 cannot be expressed as the sum of two perfect squares.

Let us discuss some examples.

1) To find N(n) for n = 100.

divisors are 1, 2, 5, 10, 20, 25, 50, 100

$$N(n) = 4 \sum_{d/n} h(d) = 4\ (1 + 1 + 1)$$

$$= 12$$

$$\therefore N(n) = 12$$

The solutions are

(6, 8) (-6, -8) (-6, 8) (-8, 6) (0, 10) (0, -10)

(8,6) (-8, -6) (8, -6) (6, -8) (10, 0) (-10, 0)

2) For n = 101

divisors are 1, 101

$$N(n) = 4 \sum_{d/n} h(d) = 4\ (1 + 1)$$

$$= 8$$

$\therefore$ N(n) = 8

The Solutions are

(1, 10) (-1, 10) (-1, -10) (1, -10) (10, 1) (10, -1)

(-10, -1) (-10, 1)

3) For n = 102

divisors are 1, 2, 3, 6, 17, 51, 102

$$N(n) = 4 \sum_{d/n} h(d) = 4(1 - 1 + 1 - 1)$$

$$= 0$$

$\therefore N(n) = 0$

SECTION - 6

In this section we shall study the paper entitled "Every integer is a sum or difference of 28 integral eighth powers" by L.N. Vaserstein.

Here the author has discussed the following problem.

Let $\tau(k)$ be theleast 'S' such that every integer is the sum of 'S' elements of the form $\pm z^k$ where z is an integer.

In this article the author has established the following.

$$17 \leq \tau(8) \leq 28$$

The first theorem proved here is as follows.

Theorem : 1.6.1

$2^{n+1} + 1 \leq \tau(2^n)$ for any integer $n \geq 2$

Proof

Modulo $2^{n+2} = 4K$, every K^{th} power Z^k is 0 or 1. Let us show that the number 6K is not a sum or differrence of 2K, K^{th} powers.

Assume the contrary

Now, $6K = 4K + 2K$ is the sum of 2K integer and either each of them is 1 modulo 4K or each of them is -1 modulo.

The second case is impossible because 6K is positive.

The first case is also impossible because $2K < 6K < 3^K$

The above theorem shows that $17 \leq \tau(8)$, this is got by taking n= 3 in the above theorem.

Exact value of $\gamma(k)$ is known only for $k = 1$ and $k = 2$.

$\gamma(1) = 1$ and $\gamma(2) = 3$

To show that $\gamma(8) \leq 28$

consider the identity

$$(a^{56} b^{31} c^{54} + b^{31} c^{110})^8$$

$$+ (a^{25} c^{116} x + a^{25} b^{88} c^{28})^8$$

$$+ (a^{25} b^{31} c^{85} x + a^{57} b^{63} c^{21})^8$$

$$- (a^{56} b^{31} c^{54} x - b^{31} c^{110})^8$$

$$- (a^{25} c^{116} x - a^{25} b^{88} c^{28})^8$$

$$- (a^{25} b^{31} c^{85} x - a^{57} b^{63} c^{21})^8$$

$$+ (a^{55} b^{25} c^{61} x - a^{7} b^{73} c^{61})^8$$

$$+ (a^{20} b c^{120} x - a^{60} b^{81})^8$$

$$+ (a^{31} b^{36} c^{74} x - a^{15} b^{63} c^{63})^8$$

$$- (a^{55} b^{25} c^{61} x + a^{7} b^{73} c^{61})^8$$

$$- (a^{20} b c^{120} x + a^{60} b^{81})^8$$

$$- (a^{31} b^{36} c^{74} x + a^{15} b^{63} c^{63})^8$$

$$= \left(16\, a^{56} b^{248} c^{120}\right) e x \text{ with}$$

$$e = c^{704} + a^{144} b^{368} c^{192} + a^{368} b^{224} c^{112}$$

$$- a^{48} b^{288} c^{368} - a^{384} b^{320} - a^{80}$$

$$b^{229} c^{395}.$$

The above identity shows that every term of a non-trivial arithmetic progression m_0^x ($m_0 \neq 0$) is the sum or difference of 12 eighth powers.

An earlier result of Fuchs and Wright (1939) show every integer is the sum or difference of 16 eighth powers modulo any given $m \neq 0$

Using this result and the above identity we obtain

$\gamma(8) \leq 12+16 = 28.$

SECTION - 7

In this section we shall discuss the paper entitled 'on equal sums of sixth powers' by Ajai Choudhry.

This paper deals with solution of the Diophantine equation $x^6 + y^6 + z^6 = u^6 + v^6 + w^6$

The author starts with the following result of Bremner.

$$\left.\begin{aligned} x^2 + xu - u^2 &= w^2 + wz - z^2 \\ y^2 + yv - v^2 &= u^2 + ux - x^2 \\ z^2 + zw - w^2 &= v^2 + vy - y^2 \end{aligned}\right\} \quad \text{I}$$

Any solution of above set of 3 equations gives a solution of the equation.

$$x^r + y^r + z^r = u^r + v^r + w^r \text{ for } r = 2, 6$$

To prove this for r = 2 it is enough to add all these equations.

To prove for r = 6 we proceed as follows.

Consider the set of equations I

Raising to the power 3 and adding all the equations we get

$$x^6 + y^6 + z^6 = u^6 + v^6 + w^6$$

In this paper the author gives a method of finding new solutions starting with a given set of solutions of

$$x^6 + y^6 + z^6 = u^6 + v^6 + w^6$$

Let a solution of $x^6 + y^6 + z^6 = u^6 + v^6 + w^6$ be given by

$x = \alpha_1$, $y = \beta_1$, $z = \Gamma_1$, $u = \alpha_2$, $v = \beta_2$, $w = \Gamma_2$,

Then a new solution is obtained by taking

$x = ap + \alpha_1 q$ $\qquad u = dp + \alpha_2 q$

$y = bp + \beta_1 q$ $\qquad v = ep + \beta_2 q$

$z = cp + \Gamma_1 q$ $\qquad w = \Gamma_2 q$

Where

$$p = -\{ a(2\alpha_1 - \alpha_2) + b(2\beta_1 + \beta_2) - d(\alpha_1 + 2\alpha_2) + e(\beta_1 - 2\beta_2)\}$$

$$q = a^2 - ad + b^2 + be - d^2 - e^2$$

and a,b,c,d,e are given as

$$a = \{(\alpha_1-\Gamma_2)^2 + 2(\alpha_1 - \Gamma_2)(\Gamma_1 - \alpha_2)\} \{(\beta_1-\Gamma_2)^2 + (\beta_1 - \Gamma_2)(\Gamma_1 - \beta_2) - (\Gamma_1 - \beta_2)^2\}$$

$$b = \{(\beta_1-\Gamma_2)^2 - 2(\beta_1 - \Gamma_2)(\Gamma_1 - \beta_2)\} \{(\Gamma_1-\alpha_2)^2 + (\Gamma_1 - \alpha_2)(\alpha_1 - \Gamma_2) - (\alpha_1 - \Gamma_2)^2\}$$

$$c = \{(\Gamma_1-\alpha_2)^2 + (\Gamma_1 - \alpha_2)(\alpha_1 - \Gamma_2) - (\alpha_1 - \Gamma_2)^2\} \{(\beta_1-\Gamma_2)^2 + (\beta_1 - \Gamma_2)(\Gamma_1 - \beta_2) - (\Gamma_1 - \beta_2)^2\}$$

$$d = -\{(\Gamma_1-\alpha_2)^2 + (\alpha_1 - \Gamma_2)^2\} \{(\beta_1-\Gamma_2)^2 + (\beta_1 - \Gamma_2)(\Gamma_1 - \beta_2) - (\Gamma_1 - \beta_2)^2\}$$

$$e = \{(\Gamma_1-\beta_2)^2 + (\beta_1 - \Gamma_2)^2\} \{(\Gamma_1-\alpha_2)^2 + (\Gamma_1 - \alpha_2)(\alpha_1 - \Gamma_2) - (\alpha_1 - \Gamma_2)^2\}$$

As an example of this procedure the author considers,

$x = 3$, $y = 22$, $z = -19$, $u = 23$, $v = 15$, $w = 10$

using this procedure the author has obtained

$x = 233$, $y = 916$, $z = -711$

$u = 939$, $v = 509$, $w = 508$

A parametric solution of this equation is given by

$$x = 2m^6 + 2m^5 + m^4 - 16m^3 + 35m^2 - 12\,m + 3$$

$$y = -m^6 + 3m^5 - 16m^4 + 27m^3 - 4m^2 - 9\,m + 5$$

$$z = 3m^6 - 2m^5 + 6m^4 + 16m^3 - 18m^2 + 14\,m + 1$$

$$u = -m^6 - 10m^5 + 14m^4 - 16m^3 - 2m^2 - 10\,m + 5$$

$$v = -3m^6 + m^5 - 4m^4 + 13m^3 + 4m^2 + m + 3$$

$$w = 2m^6 - 6m^5 - 11m^4 + 16m^3 - 25m^2 + 20\,m - 1$$

The author has obtained another set of parametric solution in the following form.

$$\alpha_1 = 3m^4 + 8m^3 + 9m^2$$

$$\beta_1 = m^4 + 3m^3 + 14m^2 + 15m + 9$$

$$\Gamma_1 = 2m^4 + 12m^3 + 19m^2 + 18m + 9$$

$$\alpha_2 = -2m^4 - 4m^3 + 5m^2 + 12m + 9$$

$$\beta_2 = 3m^4 + 9m^3 + 18m^2 + 21m + 9$$

$$\Gamma_2 = m^4 + 10m^3 + 17m^2 + 12m$$

Chapter II

CHAPTER - 2

SECTION - 1

GENERAL INFORMATION ON EULER'S ϕ FUNCTION.

$\phi(n)$ is defined to be number of positive integers $\leq$ n and relatively prime to n. We shall collect some important properties of the function $\phi(n)$.

Theorem 2.1.1:

$$\sum_{d/n} \phi(d) = n$$

Proof

Let $S = \{ 1,2,3, \ldots\ldots n\}$

If d is a divisior of n,

Let $A(d) = \{ K/K \in S , (n,k) = d\} \subseteq s$

Suppose $d_1 \neq d_2$ then $A(d_1) \neq A(d_2)$

$A(d_1) \cap A(d_2) = \phi$

$$S = \bigcup_{d/n} A(d)$$

Let f(d) be the number of elements in A(d)

$$n = \sum_{d/n} f(d)$$

$K \in A(d) \iff (n,k) = d$

$$\iff \left[\frac{A}{d} , \frac{K}{d} \right] = 1$$

$\Leftrightarrow$ (K/d) is relatively prime to (n/d)

$(K/d) \leq (n/d)$

$\therefore f(d) = \phi(n/d)$

$$n = \sum_{d/n} f(d) = \sum_{d/n} \phi(n/d)$$

$$= \sum_{d/n} \phi(d)$$

Remark : 2.1.2

The mobius function μ is defined as

$\mu(1) = 1$

If $n>1$, $n = P_1^{a_1} \ldots\ldots\ldots P_k^{a_k}$

then $\mu(n) = (-1)^k$ if $a_1 = a_2 = \ldots = a_k = 1$

$\mu(n) = 0$ otherwise

An important property of $\mu(n)$ is given as

If $n \geq 1$ we have

$$\sum_{d/n} \mu(d) = \begin{bmatrix} 1 \\ \vdots \\ n \end{bmatrix} = \begin{cases} 1 \text{ if } n = 1 \\ 0 \text{ if } n > 1 \end{cases}$$

Theorem: 2.1.3

$$\phi(n) = \sum_{d/n} \mu(d) \frac{n}{d}$$

Proof

$$\phi(n) = \sum_{k=1}^{n} \left[\frac{1}{(n,k)} \right]$$

$$\sum_{k=1}^{n} \left[\frac{1}{(n,k)} \right] = 0 \text{ if } (n,k) > 1$$

$$\sum_{k=1}^{n} \left[\frac{1}{(n,k)} \right] = 1 \text{ if } (n,k) = 1$$

$$\phi(n) = \sum_{k=1}^{n} \left[\frac{1}{(n,d)} \right] = \sum_{k=1}^{n} \left(\sum_{d/(n,k)} \mu(d) \right)$$

$$= \sum_{k=1}^{n} \sum_{\substack{d/n \\ d/k}} \mu(d) = \sum_{d/n} \sum_{q=1}^{n/d} \mu(d) = \sum_{d/n} \mu(d) \frac{n}{d}$$

Product formula for $\phi(n)$

Theorem: 2.1.4

$$\phi(n) = n \prod_{p/n} (1 - 1/p)$$

Proof $n = P_1^{\alpha_1} \ldots\ldots\ldots P_r^{\alpha_r}$

$$\prod_{i=1}^{r} (1 - 1/p_i) = 1 - \sum \frac{1}{P_i} + \sum \frac{1}{P_i P_j} + \ldots\ldots$$

$$\ldots\ldots\ldots\ldots\ldots + (-1)^r \frac{1}{P_1 P_2 \ldots P_r}$$

$$= 1 + \sum \frac{\mu(P_i)}{P_i} + \sum \frac{\mu(P_iP_j)}{P_iP_j} + \ldots + \frac{\mu(P_1 \ldots P_r)}{P_1 \ldots P_r}$$

$$\phi(n) = \sum_{d/n} \mu(d) \frac{n}{d} = n \sum_{d/n} \frac{\mu(d)}{d}$$

$\mu(d)$ is not 0 only when $d = 1$ and

$$d = \begin{cases} P_1, P_2, P_3 \ldots\ldots\ldots P_r \\ P_iP_j \qquad i = 1,2, \ldots\ldots r;\ j = 1,2, \ldots\ldots r;\ i \neq j \\ P_i P_j P_k \qquad i,j,k = 1,2 \ldots r;\ i \neq j \neq k \\ \vdots \\ P_1 \ldots\ldots P_r \end{cases}$$

$$\sum \frac{\mu(d)}{d} = 1 + \sum \frac{\mu(P_i)}{P_i} + \sum \frac{\mu(P_iP_j)}{P_iP_j} + \ldots + \frac{\mu(P_1 \ldots\ldots P_r)}{P_1 \ldots\ldots P_r}$$

$$= \prod_{i=1}^{r} (1 - 1/p_i)$$

$$\therefore \phi(n) = n \prod (1 - 1/p_i)$$

Using the product formula the following properties of ϕ can be easily proved.

1. $\phi(P^n) = P^n - P^{n-1}$ if P is a prime

2. $\phi(mn) = \phi(m)\ \phi(n)\ \frac{d}{\phi(d)}$ where $d = (m,n)$

3. $\phi(mn) = \phi(m)\ \phi(n)$ if $(m,n) = 1$

4. $a/b \Rightarrow \phi(a) / \phi(b)$

We shall discuss the following problems.

a) When $n = 2^r$

$\phi(n) = 2^{r-1}(2-1) = 2^{r-1} = n/2$

$\therefore \phi(n) = n/2$

b) When n is odd

$\phi(2n) = \phi(2)\ \phi(n)$

$= \phi(n)$

c) $\phi(n) = 12$ when $n = 13,\ n = 26$

Definition : 2.1.4

A function F is said to be multiplicative if $f \not\equiv 0$ and if

$f(mn) = f(m)\ f(n)$ if $(m,n) = 1$

ϕ is multiplicative

Definition : 2.1.5

A function f is completely multiplicative if $f \not\equiv 0$ and

$f(mn) = f(m)\ f(n)$

ϕ is not completely multiplicative.

SECTION - 2

In this section we shall discuss the paper "An inequality for Euler's totient function" by A.M. Vaidya

The main theorem proved here is stated as follows

Theorem : 2.2.1

For all natural numbers n except n=2 and n = 6

$\phi(n) \geq \sqrt{n}$

Where ϕ (n) is the Euler's totient function

Lemma 2.2.2

If $f(x) = x^n - x^{n-1}$, where $n \geq 1$

then

(a) $f(x) \geq 1$ for $x \geq 2$ and

(b) $f(x) > \sqrt{2}$ for $x \geq 3$

Proof

We have

$f'(x) = nx^{n-1} - (n-1)\, x^{n-2} > 0$, for $x \geq 2$

Hence f (x) is increasing for $x \geq 2$

Since f (2) $\geq$ 1 and f (3) $> \sqrt{2}$

Lemma 2.2.3

If P is a prime then $\phi(P^r) \geq P^{r/2}$

except when $P^r = 2$ (ie) when P = 2 and r = 1

Proof

Case - 1

$r = 1$ and P odd

$\phi(P^r) = \phi(P) = P - 1 \geq \sqrt{P}$

if $(P-1)^2 \geq P$

(ie) if $P^2 - 3P + 1 \geq 0$

(ie) if $P \geq \frac{3 + \sqrt{5}}{2}$

(ie) if $P \geq 3$ which is true

Case - 2 $r \geq 2$

$\phi(P^r) = P^r - P^{r-1} \geq P^{r/2}$

if $P^{r/2} - P^{(1/2)\,r-1} \geq 1$

and for $P \geq 2$, $r \geq 2$ this is true by Lemma 2.2.2

Lemma 2.2.4

1) $\phi(2P^k) \geq \sqrt{2p}$, if $k>1$, p an odd prime

$\phi(2P) \geq \sqrt{2p}$ if $P>3$ is a prime

Proof

(1) $\phi(2P^k) = \phi(P^k) = P^k - P^{k-1} \geq \sqrt{2}\ P^{(1/2)k}$

if $P^{(1/2)k} - P^{(1/2)k-1} \geq \sqrt{2}$

and this is true for $P \geq 3$ by lemma - 1

(2) $\phi(2P) = \phi(P) = P-1 \geq \sqrt{2p}$

if $(P-1)^2 \geq 2P$

(ie) if $P^2 - 4P + 1 \geq 0$

(ie) if $P \geq 2 + \sqrt{3}$

(ie) if $P \geq 5$, which is true.

Proof of the theorem 2.2.1.

Since the function $\phi(n)$ and $\sqrt{n}$ are multiplicative the proof follows from lemma 2.2.3 and 2.2.4.

SECTION - 3

In this section we shall discuss the paper entitled "An extension of Euler's function" by P.Kesava Menon

Here the author has introduced a new extension of Euler's function denoted by $\phi_f(n)$ and establishes a number of applications for these results.

Consider a polynomial f(x) with integral Co-efficients for each n. $\boldsymbol{\phi_f(n)}$ is defined to be the number of residues x mod n for which f(x) is prime to n

Consider the following examples

1) $f(x) = x^2 + 1,\ n = 7$

$\therefore\ \phi_f(7) = 7$

2) $f(x) = x^2 + 1,\ n = 6$

$\therefore\ \phi_f(6) = 3$

3) $f(x) = x^2 + 5,\ n = 11$

$\therefore\ \phi_f(11) = 11$

4) $f(x) = x^2 + 5,\ n = 13$

$\therefore\ \phi_f(13) = 13$

5) $f(x) = x^2 + 9,\ n = 11$

$\therefore\ \phi_f(11) = 11$

6) $f(x) = x^2 + 9,\ n = 5$

$\therefore\ \phi_f(5) = 3$

We can show that the function $\phi_f(n)$ has many of the properties of the function $\phi(n)$

Definition: 2.3.1.

Given a prime P and a polynomial f with integral Co-efficients, let $\mathbf{f_p}$ denote the number of distinct roots of the congruence $f(x) \equiv 0 \pmod{P}$

Consider the following examples.

1) $f(x) = x^2 + 1$, $P = 5$

$\therefore f_p = 1$

$f(x) = (x+1)(x+2) = x^2 + 3x + 2$, $P = 3$

$\therefore f_p = 2$

The three important theorems proved in this article are as follows.

Theorem 2.3.2.

The function ϕ_f (n) is multiplicative

Proof

Let (m,n) = 1.

a,b be a pair of numbers belonging respectively to a complete residue system mod m and a complete residue system mod n such that f(a), f(b) are prime to m,n respectively.

Then there is a unique number c in any complete residue system mod m satisfying the relations.

$c \equiv a \bmod m \qquad c \equiv b \bmod n$

such that $f(c)$ is prime is mn

conversely

Given any c mod mn for which $f(c)$ is prime to mn there is a unique pair a,b belonging respectively to any complete residue system mod m and any complete residue system mod n such that $f(a)$, $f(b)$ are prime to m,n respectively, it follows that

$$\phi_f(mn) = \phi_f(m)\ \phi_f(n)$$

Theorem : 2.3.3.

The value of $\phi_f(n)$ is given by

$$\phi_f(n) = n \prod_{p/n} (1 - f_p/P) \text{----------(1)}$$

Where the product is over all distinct prime factors P of n and f_p denotes the number of distinct roots of the congruence

$$f(x) \equiv 0 \pmod P$$

Proof

By a repeated application of theorem 2.3.2

We have $\phi_f(n) = \prod_{p} \phi_f(P^r)$ ---------- (2)

Where $\prod_{p/n} P^r$ is the unique decomposition of

n into prime factors

Therefore the problem reduces to evaluating $\phi_f(P^r)$ for $r \geq 1$.

Since f(x) is prime to P^r ($r \geq 1$) for a certain value of x iff it is prime to P for the same value of x. We have to find the number of numbers among the set

$$a = a_0 + a_1 P + \ldots\ldots + a_{r-1} P^{r-1},$$

$$0 \leq a_i \leq P-1, \quad (i = 0,1 \ldots r-1) \text{ ----------(3)}$$

for which f(a) is prime to P . Now obviously f(a) is prime to P if and only if $f(a_0)$ is prime to P.

In other words, there is only a restriction on the choice of the value of a_0 and the remaining a_i may be choosen arbitrarily.

The number of values of a_0 for which $f(a_0)$ is prime to P is equal to $P - f_p$ where f_p is the number of distinct solutions of the congruence.

$$f(x) \equiv 0 \pmod{p}$$

Hence $\phi_f(P^r) = P^{r-1} (P - f_p) = P^r (1 - f_p/P)$ ----- (4)

Substituting from (4) in (2) we get (1)

$$\therefore \phi_f(n) = n \prod_{p/n} (1 - f_p/P)$$

Applications of theorem 2.3.2 and 2.3.3

Theorem : 2.3.4

Let $S : \{ m_1, \ldots\ldots m_r\}$ be a given set of numbers and let N(p) be the number of distinct residues modP among them for any prime P. Then the number of sequence.

$$a+m_1,\ a+m_2 \ldots\ldots\ a+m_r \pmod n \qquad \text{---------- (1)}$$

in which all terms are prime to n is equal to

$$n \prod_{p/n} \{1- N(p)/P\} \qquad \text{---------- (2)}$$

Proof :

Take $f(x) = (x+m_1)\ (x+m_2) \ldots\ldots\ (x+m_r)$ ---------- (3)

in theorem 2.3.3

Obviously f(x) is prime to n for a certain value of x iff if each individual factor

$$x + m_i \ (i = 1, \ldots\ldots r)$$

is prime to n for the same value of x so that the number of sequence (1) having the requistic property is the same as the number of values x mod n for which the polynomial (3) is prime to n. Let for any prime factor P of n

$$n_1,\ n_2 \ldots\ldots\ n_\tau \qquad (\tau = N(p)) \text{ ------- (4)}$$

be the distinct residues mod p among

$$m_1,\ m_2,\ \ldots\ldots\ldots\ m_r$$

Then for

$$x \equiv -n_i \mod P \quad (i = 1,2 \ldots\ldots\ldots \tau)$$

and for these values only, will the function f(x) take the value O modP so that f_p in theorem 2.3.3. is equal to τ from which the theorem follows.

Some interesting special cases of theorem 2.3.4.

Proposition 2.3.5

If the prime factors of n are greater than the prime factors of all numbers of the set.

$$S : \{m_1, \ldots\ldots m_r\}$$

then the number of sequence (1) in theorem 2.3.4 in which all terms are prime to n is

$$n \prod_{p/n} (1 - r/P)$$

Proposition - 2.3.6

If the prime factors of n are all greater than the number of the set

$$\bar{S} : \{m_1, \ldots\ldots m_{r-1}\}$$

then the number of sequence

$$a, a+m_1, \ldots\ldots a+m_{r-1} \pmod n$$

in which the terms are all prime to n is equal to

$$n \prod_{p/n} (1-r/p)$$

Proposition : 2.3.7

If for a prime P, $(r, P-1) = a_p$ then the number of numbers x^r-1 which are prime to n, when x runs through a complete residue system modn is

$$n \prod_{p/n} (1-a_p/P)$$

Proposition : 2.3.8

If for a prime P, $(r-1, P-1) = b_{p-1}$ then the number of numbers x^r-x which are prime to n when x runs through a complete residue system modn is

$$n \prod_{p/n} (1-b_p/P)$$

Proposition : 2.3.9

If d is not a perfect square then the number of numbers x^2-d that are prime to n as x runs through a complete system of residues modn is equal to

$$n \prod_{p/n} (1-d_p/p)$$

where d_p is defined for all prime p by

$$d_p = \begin{cases} 1 & \text{if } d \equiv o \pmod{p}, \text{ or if } p = 2 \\ 2 & \text{if p is odd and d is a quadratic residue mod p} \\ 0 & \text{if p is odd and d is a quadratic non-residue mod p} \end{cases}$$

Before we state the next theorem we need the following definition

Definition : 2.3.10

$$\text{when } n = \pi_{p/n} p^r$$

$$\tau_f(n) = \pi_{p/n} f_p^r$$

Theorem 2.3.11

If $\tau_f(n)$ is defined for all n by

$$\tau_f(n) = \pi_{p/n} f_p^r \quad , \quad n = \pi_{p/n} p^r$$

where f_p denotes the number of distinct solutions of

$$f(x) \equiv o \pmod{p}$$

for all primes p then

$$\sum_{d/n} \phi_f(d)\, \tau_f(n/d) = n \quad \text{---------- (1)}$$

Proof

It is easily seen that the left hand side of (1) is equal to

$$\pi_{p/n} \sum_{r=0}^{t} \phi_f(P^r)\, \tau_f(P^{t-r})$$

We have to show that

$$\sum_{r=0}^{t} \phi_f(P^r)\, \tau_f(P^{t-r}) = P^t \quad \text{---------- (2)}$$

The left hand side of (2) is equal to

$$\sum_{r=0}^{t} \phi_f (P^r)\, \psi_f (P^{t-r}) = \sum_{r=0}^{t} \phi_f (P^r)\, f_p{}^{t-r}$$

$$= f_p{}^t + \sum_{r=1}^{t} P^{r-1} (P-f_p)\, f_p{}^{t-r}$$

$$= f_p{}^t + (P-f_p) \sum_{r=1}^{t} P^{r-1}\, f_p{}^{t-r}$$

$$= f_p{}^t + (P-f_p) \{f_p{}^t + P^1 f_p{}^{t-1} + P^2 f_p{}^{t-2} + \ldots\ldots\ldots + P^{t-1}\}$$

$$\therefore \sum_{r=0}^{t} \phi_f (P^r)\, \psi_f (P^{t-r}) = P^t$$

SECTION - 4

In this section we shall study the paper "On extension of Euler's ϕ function" by Nageswara Rao.

Here also the author is able to generalize all well known properties of the Euler's totient function to the new extension of Euler's function introduced by him.

We shall start with the priliminary definitions.

Definition : 2.4.1

If K is any integer ≥ 1 and A,B are any two integer not both zero then $(A,B)_K$ denotes the largest common divisor of A and B which is also a K - th power.

Definition : 2.4.2

Given positive integers K and M, $\phi_K(M)$ is the number of non-negative integers x less than M^K such that $(x,M^K)_K = 1$.

Just as in the case of Euler's ϕ function we have to use the principle of cross classification to prove the product formula for $\phi_K(M)$.

Principle of cross classification

Let S be a set, let S_1, S_2, ... S_n be subsets of S.

Let N(S) denote the number of elements S then

$$N\left(S - \bigcup_{i=1}^{n} S_i\right) = N(S) - \sum_{i=1}^{n} N(S_i) + \sum_{\substack{i,j=1 \\ i \neq j}}^{n} N(S_i\, S_j)$$

$$- \Sigma\, N(S_i\, S_j\, S_k) + \ldots + (-1)^n\, N(S_1 \ldots S_n)$$

A product formula for $\phi_K(M)$

Theorem : 2.4.3

$$\phi_K(M) = M^K (1-1/P_1)^K\, (1-1/P_2)^K \ldots\ldots (1-1/P_t)^K$$

Where P1, P2, ... Pt are all distinct prime factors of M

Proof:

ϕ_K (M) is equal to the number of numbers $< M^K$ and which are not divisible by Prime powers P_1^K . . . . . P_r^K where

$M = P_1, P_2 \ldots\ldots P_r$

Let S = 1, 2, ... M^K

Let S_i = the set of numbers in S which are divisible by P_i^K

$$\phi_K(M) = N\left(S - \bigcup_{i=1}^{r} S_i\right)$$

Using the principle of cross classification

we get

$$\phi_K(M) = M^K - \Sigma\, \frac{M^K}{P_i^K} + \Sigma\, \frac{M^K}{P_i^K\, P_j^K} - \ldots\ldots$$

Hence

$$\phi_K(M) = M^K\, (1-1/P_1^K)\, (1-1/P_2^K) \ldots (1-1/P_t^K)$$

Theorem : 2.4.4

If d is a divisor of M, K reduced residue system (mod M) can be decomposed into $\phi_K(M)/\phi_K(d)$, K - reduced residue system (mod d)

The proof of the theorem is exactly similar to the proof of the following well known theorem,

Theorem 2.4.5

Given integers r,d,K such that d/K and (r,d) = 1 then the number of elements in the set {r+td/t= 1,2 ..... K/d} which are relatively prime to K is $\phi(K)/\phi(d)$

Proof

Let P be a prime

Suppose P/K P/r+td P/d

=> p/r

∴ p/K, p/r+td for some t

=> p ∤ d

Let S = { r+td /t = 1,2 ..... K/d}

We want N (s-t)

Where T = { x ∈ s / (x,K) > 1}

Let $P_1, P_2, \ldots P_r$ be the primes which divide K and which do not divide d

x ∈ T => x = r+td

P_i/x for some i

$$K' = P_1 \ldots\ldots P_r$$

$$S_1 = \{ X \in S / (P_i/x) \}$$

$$S_i = \{ X \in S / (P_i/x) \}$$

$$T = \bigcup_{i=1}^{r} S_i$$

$$r + td \equiv O \pmod{P_i}$$

Pi $\nmid$ d there exist a unique t in $[1,P_i]$ such that $td \equiv -r \pmod{Pi}$ there exist a unique t in each of the intervals

$$[1,P_i]\ [P_{i+1}, 2P_i] \ldots\ldots [(q-1)\ P_{i+1}, qP_i]$$

where $qP_i = K$

$$N(S_i) = K/P_i$$

$$\therefore N(S - US_i) = N(S) - \Sigma N(S_i) + \ldots\ldots\ldots$$

$$= \frac{K}{d} - \Sigma \frac{K}{dP_i} + \Sigma \frac{K}{dP_iP_j} - \ldots\ldots\ldots\ldots$$

$$= \frac{K}{d} \cdot \frac{\prod_{p_i/K} (1-1/p_i)}{\prod_{p_i/d} (1-1/p_i)} = \frac{\phi(K)}{\phi(d)}$$

using the above two results the author discusses the number of solutions in xy of the co-gruence $N \equiv x+y \pmod{M^K}$

Where $(X, M^K)_K = 1 = (y, M^K)_K$

Regarding this problem the author has obtained the following results.

Result : 2.4.6

If N is a given number K - prime to M^K, the number of numbers N', K prime to M^K satisfying $N+N' \equiv 0 \pmod{d^K}$ is $\phi_K(m)/\phi_K(d)$

Result : 2.4.7

If N is an integer such that $(N,M^K)_K = d^K$ then the number of solution (mod M^K) of the congruence.

$N \equiv x,y \pmod{M^K}$ where $(x,M^K)_K = 1 = (y,M^K)_K$

is $\phi_K(M) \prod_p (1-1/[P^K - 1])$

The product extending over the prime factors of M/d which do not occur in d.

The author extends $\phi_K(M)$ and defines $\phi_K^{(s)}(M)$

Definition : 2.4.8

$\phi_K^{(s)}(M)$ - For positive integers K,S and M to be the number of sets of S consecutive integers each less than and relatively K - prime to M^K.

He has obtained the product formula for $\phi_K^{(s)}(M)$ in the following theorem.

Theorem : 2.4.9

$$\phi_K^{(s)}(M) = M^K (1-[s/p_1^K])$$

$(1-[s/P_2^K]) \ldots\ldots\ldots\ldots (1-[s/p_t^K])$ where P1,P2, . . . Pt are all the distinct prime factors of M and $P_i^{K>s}$ $(i = 1,2, \ldots\ldots t)$

A further extension of $\phi_K^{(s)}(M)$ is defined as follows.

$$\phi_K^{(s)}(M) = M^K [1-(S/P_1^K)] [1-S/P_2^K)] \ldots\ldots [1-(S/P_t^K)]$$

Theorem: 2.4.10.

$$\phi_K(M;A) = M_1^K [1- \lambda_1/P_1^K)] [1- \lambda_2/P_2^K)] \ldots\ldots$$

$$[1- \lambda_t/P_t^K)]$$

Where P_1, P_2, ... P_t are all the distinct prime factors of M and λi is the number of distinct residues (mod Pi^K) $(i = 1,2, \ldots\ldots t)$ of the integers in A.

Summary and Conclusion

SUMMARY AND CONCLUSION

In this thesis we have attempted to study some important Diophantine equations and two interesting extensions of the Euler's ϕ function.

The Diophantine equations studied here are as follows

1) Integral solutions of the Diophantine equation $ax + by = c$.

2) The Diophantine equation $X^2 + Y^2 = Z^2$.

3) Expressing every positive integer as a sum of four squares and as a sum of five positive squares.

4) Waring's problem.

5) Given n to find the number of solutions of the equation $x^2 + y^2 = n$.

6) Every integer is a sum or difference of 28 integral eighth powers.

7) Solutions of the Diophantine equation
$x^6 + y^6 + z^6 = u^6 + v^6 + w^6$

In the year 1967 P. Kesava Menon has defined the concept of $\phi_f(n)$ an extension of Euler's totient function $\phi(n)$.

In the year 1961 Nageswara Rao defined another extension $\phi_K(M)$ of the concept of $\phi(n)$

These two concepts are studied in detail in these two papers. We find that all the properties of $\phi(n)$ can be generalize to the new function $\phi_f(n)$ and $\phi_K(M)$. further Kesava Menon has obtained some interesting applications of the function $\phi_f(n)$

We want to conclude this thesis with the following two quotations.

"Mathematics when rightly viewed pocessess not only truth but supreme beauty-sublimely pure and capable of stern perfection such as only a greatest art can show".

– **BERTRAND RUSSEL**

"Mathematics is in many ways the most elaborated and sophisticated branch science-ladder for mystical as well as rational thought in the intellectual ascent of man".

– **JACOB BRONOWSKI**

Bibliography

BIBLIOGRAPHY

1) AJAI CHOUDHRY — "On equal sums of sixth powers", Indian Journal of Pure and Applied Mathematics, 25,(1994), 837-841.

2) ALBERT FASSLER — "Multiple pythagorean number triples", American Mathematical Monthly, (1991), 505-517.

3) HARDY G.H & WRIGHT E.M. — "An introduction to the theory of numbers", The English Language Book Society and Oxfort University Press.

4) HONSBERGER — "Ingenuity in Mathematics", New Mathematical Library, Mathematical Association of America Washington, 23, (1970), 27-31.

5) KESAVA MENON P. — "An extension of Euler's function", The Mathematics Student, 35, (1967), 55-60.

6) LAMBEK J. & MOSER L. — "On the distribution of Pythagorean triangles", Pacific J. Math, 5,(1955), 73-83.

7) NAGESWARA RAO K. — "On extension of Euler's ϕ function", The Mathematics Student, 29, (1961), 121-126.

8) VAIDYA A.M. "An inequality for Euler's totient function", The Mathematics Student, 35, (1967), 79-80.

9) VASERSTEIN L.N. "Every integer is a sum or difference of 28 integral eighth powers", Journal of Number Theory, 28, (1988), 66-68.

10) WALLAW SIERPINSKI "A selection of problems in the theory of numbers", P.W.N - Polish Scientific Publishers Warzawa (1964), 104-120.