International Journal of Current Research and Modern Education (IJCRME)
ISSN (Online): 2455 - 5428
(www.rdmodernresearch.com) Volume I, Issue I, 2016

A STUDY ON NUMBER THEORY AND ITS APPLICATIONS

A. Dinesh Kumar*, M. Vasuki & K. Jeyabal***
* Assistant Professor, Department of Mathematics, Dhanalakshmi Srinivasan Engineering College, Perambalur, Tamilnadu
** Assistant Professor, Department of Mathematics, Srinivasan College of Arts and Science, Perambalur, Tamilnadu

Introduction:

Number theory, also known as higher arithmetic is a branch of mathematics concerned with the properties of integers, rational numbers, irrational numbers and real numbers. Sometimes the discipline is considered to include the imaginary and complex numbers as well.

Formally, numbers are represented in terms of sets; there are various schemes for doing this. However, there are other ways to represent numbers. As angles, as points on a line, as on a plane or as points in space. The integers and rational numbers can be symbolized and completely defined by numerals. The system of numeration commonly used today was developed from systems used in Arab texts, although some scholars believe they were first used in India. The so-called Arabic numerals are $0, 1, 2, 3, 4, 5, 6, 7, 8$ and 9

Number theory is one of the oldest branches of pure mathematics and one of the largest of course; it concerns questions about numbers, usually meaning whole numbers or rational numbers. Elementry number theory involves divisibility among integers… the division "algorithm", the Euclidean algorithm, elementary properties of primes, congruences, including Fermat's Little theorem and Euler's theorem extending it. But the term "elementary" is usually used in this setting only to mean that no advanced tools from other areas are used… not that the results themselves are simple. Indeed, a course in "elementry" number theory usually includes classic and elegant results such as Quadratic Reciprocity; counting results using the Mobius Inversion Formula; and even the prime number theorem, asserting the approximate density of primes among the integers, which has difficult but "elementry" proofs. In such chapter we shall discuss the topic of representing positive integers as sum of squares of two or more integers.

Some Basic Definitions and Sum of Two Squares:

Integers: The numbers $0, 1, -1, 2, -2, 3, -3$ … are called integers of which $1, 2, 3, \ldots$ are called positive integers and $-1, -2, -3, \ldots$ are called negative integers. The collection of all integers is denoted by Z. Thus $Z = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$

Natural Numbers: The numbers $1, 2, 3, \ldots$ are called natural numbers. They are also called counting numbers. Since, they are used for counting objects. The collection of all natural numbers is denoted by N. Thus $N = \{1, 2, 3, \ldots\}$

Least Common Multiple: The integers $a_1, a_2, \ldots, a_n$ all different from zero, have a common multiple *'b'* if a_i / b for $i = 1, 2, \ldots, n$. The least of the positive common multiples is called the least common multiple and is denoted by $[a_1, a_2, \ldots, a_n]$

Greatest Common Divisor: The integers *'a'* is a common divisor of *'b'* and *'c'* in case a/b and a/c. Since there is only a finite number of divisors of any non-zero integer, there is only a finite number of common divisors of *'b'* and *'c'*, except in the case $b = c = 0$. If at least one of *'b'* and *'c'* is not 0.The greatest among their common divisors is called greatest common divisor of *'b'* and *'c'* and is denoted by (b, c). Similarly, We denote the greatest common divisor *'g'* of the integers $b_1, b_2, \ldots, b_n$ not all zero by $(b_1, b_2, \ldots, b_n)$

Relatively Prime: We say that *'a'* and *'b'* are relatively prime incase $(a, b) = 1$, and that $a_1, a_2, \dots, a_n$ are relatively prime incase $(a_1, a_2, \dots, a_n) = 1$. We say that $a_1, a_2, \dots, a_n$ are relatively prime in pairs in case $(a_i, a_j) = 1$ for all $i = 1, 2, 3, \dots, n$ with $i \neq j$.

Congruence: If an integer *'m'*, not zero, divides the difference $a - b$, we say that *'a'* is congruent to *'b'* modulo *'m'* and write $a \equiv b \ (mod\ m)$

Division Algorithm: Given any integers *'a'* and *'b'* with $a \neq 0$,there exist unique integers *'q'* and *'r'* such that $b = qa + r, 0 \leq r < a$.Ifa/b, then *'r'* satisfies the stronger inequalities $0 < r < a$.

Prime Number: An integer $P > 1$ is called a prime number (or) a prime in case there is no divisor *'d'* of *'p'* satisfying $1 < d < p$.If an integer $a > 1$ is not a prime. It is called a composite number.

Lattice Points: The co-ordinates of the points are an integer is called lattice points.

Sum of Two Squares:

We begin with the question of representing a given integers as the sum of two squares.

For Example

$$13 = 2^2 + 3^2$$
$$29 = 2^2 + 5^2$$
$$313 = 12^2 + 13^2$$
$$205 = 3^2 + 14^2 = 6^2 + 13^2$$

Result

$$(a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2 = (ac - bd)^2 + (ad + bc)^2$$

Theorem:

If N divides $A^2 + 1$ for some A, then N is representable as the sum of two squares.

Proof:

Let $\frac{A}{N}$ be converted into a continued fraction and let $\frac{p_n}{q_n}$ be the n^{th} congruent to $\frac{A}{N}$

Such that $q_n \leq \sqrt{N} < q_{n+1} \dots\dots\dots\dots\dots\dots (1)$

Then we have $\left|\frac{A}{N} - \frac{p_n}{q_n}\right| < \left|\frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n}\right| = \frac{1}{q_n\, q_{n+1}}$

This reduces to $|Aq_n - Np_n| < \frac{N}{q_{n+1}}$

Hence from (1) $(Aq_n - Np_n)^2 < \frac{N^2}{q_{n+1}^2} < N$

Also $q_n^2 \leq N$

$\therefore\ q_n^2 + (Aq_n - Np_n)^2 < 2N$

But, $q_n^2 + (Aq_n - Np_n)^2 = q_n^2(A^2 + 1) - 2NAp_nq_n + N^2\, p_n^2$

Which is a multiple of N, since N divides$A^2 + 1$. Thus it is proved that $q_n^2 + (Aq_n - Np_n)^2$is a multiple of N less than $2N$. This implies, $q_n^2 + (Aq_n - Np_n)^2 = N$

Hence the theorem is proved.

Result: Let N divides $A^2 + 1$ for some A, and let $\frac{p_n}{q_n}$ be a continued fraction convergent of $\frac{A}{N}$ such that $q_n \leq \sqrt{N} < q_{n+1}$ Then $N = q_n^2 + \left(\sqrt{N - q_n^2}\right)^2$

Theorem: (Euler Theorem)

If an integer N can be represented as the sum of two squares in two different ways, then N is complete.

Proof:

Without loss of generality, we assume that N is an odd integer.

$$\text{Let } N = x^2 + y^2 = u^2 + v^2 \dots\dots\dots\dots\dots\dots (1)$$

Obviously one of x & y and one of u & v is odd and the other even. We assume x & u are odd and y & v are even. … … … … … … … (2)

From (1) we obtain $x^2 - u^2 = v^2 - y^2$

Hence, $(x-u)(x+u) = (v-y)(v+y)$ … … … … … … … (3)

Let $(x-u, v-y) = d$. Since $x-u$ and $v-y$are both even integers it follows that 'd'is even. … … … … … … … (4)

Let $x-u = ad$ and $v-y = bd$ … … … … … … … (5)

For some integers 'a' and 'b'. Then $(a,b) = 1$

From (3) and (5) we obtain $a(x+u) = b(v+y)$ … … … … … … … (6)

This implies $b/x+u$ and $a/v+y$.

Hence $x+u = bt$ for some integer 't' … … … … … … … (7)

Then from (6) we get $v+y = at$ … … … … … … … (8)

It follows, since $(a,b) = 1$, that 't' is the G.C.D of $x+u$ and $v+y$ which are both even integers. ∴ 't'is even… … … … … … … (9)

Thus finally we have $4N = 2x^2 + 2y^2 + 2u^2 + 2v^2 = (x-u)^2 + (x+u)^2 + (v-y)2 + (v+y)2 = a2d2 + b2t2 + b2d2 + a2t2 = (a2+b2)(d2+t2)$

Thus $N = \{(d/2)^2 + (t/2)^2\}(a^2 + b^2)$

The theorem is therefore established since 'd' and 't' are even integers.

Theorem:

Every prime 'p' of the form $4k+1$ can be represented uniquely as the sum of two squares.

Proof:

Since'p'is of the form $4k+1, -1$ is a quadratic residue of 'p'

Hence there exists an integer A such that $A^2 \equiv -1 \ (mod\ p)$

In other words this means 'p' divides $A^2 + 1$for some A. It follows by theorem (1.1) that 'p'is representable. Now if there were two or more different representations of 'p',then by theorem. ∴ 'p' would be a composite number which is absurd. Hence the representation is unique.

Theorem:

Let N be canonically decomposed. Then N is representable if and only if every prime of the form $4q+3$ occurring in the decomposition has an even exponent.

Proof:

Necessary Part:

Given: Every prime of the form $4q+3$ occurring in the decomposition has an even exponent. To prove that N is representable. $N = n^2 p_1 p_2 \dots \dots \dots p_k$ where'n' is some integer, and $p_1, p_2, \dots \dots \dots p_k$ are all distinct primes of the form $4q+1$ (or) 2. Now we know that $n^2, p_1, p_2, \dots \dots \dots p_k$are all representable integers. Hence their product which is N is also representable.

Sufficient Part:

Given: N is representable. To prove that: Every prime of the form $4q+3$ occurring in the decomposition has an even exponent. $N = x^2 + y^2$ for some integers 'x' and 'y'. If $(x,y) = d$ and $x = x_1 d,\ y = y_1 d$ then $N = d^2(x_1^2 + y_1^2)$ … … … … … … … (1)

Such that $(x_1, y_1) = 1$. Let 'p' be any prime divisor of $x_1^2 + y_1^2$. This implies $x_1^2 + y_1^2 \equiv 0 \ (mod\ p)$ … … … … … … … … (2)

Since x_1 is prime to y_1, 'p' is relatively prime to y_1 (and x_1 also) It follows that there exists an integer 'a' satisfying the congruence

$ay_1 \equiv 1 \ (mod\ p)$ … … … … … … … (3)

Such that $(a,p) = 1$. Also multiplying (2) by a^2 we get $(ax_1)^2 + (ay_1)^2 \equiv 0 \ (mod\ p)$.

From (3) this reduces to $(ax_1)^2 + 1 \equiv 0 \ (mod\ p)$.

Thus -1 is a quadratic residue of $'p'$. $\therefore$ $'p'$ is either 2 or a prime of the form $4k+1$.

So, $x_1^2 + y_1^2$ is the product of such primes only. But, $N = d^2(x_1^2 + y_1^2)$

Hence every prime of the form $4q+3$ occurring in the decomposition of Nhas an even exponent.

Theorem: (Euler Theorem)

Let $'p'$ be a prime of the form $4q+1$. Then there exist two integers x and h such that $x^2 + 1 = hp$ where $o < x < \frac{P}{2}$ and $o < h < p$.

Proof:

$'p'$ is of the form$4q+1$. Hence-1 is a quadratic residue of $'p'$. But we know that the q_{rs} (quadratic residues) of $'p'$are

$$1^2, 2^2, \ldots\ldots\ldots \left(\frac{p-1}{2}\right)^2 \ldots\ldots\ldots\ldots\ldots\ldots (1)$$

So, -1 is congruent to one of these integers say x^2 This means $x^2 \equiv -1\ (mod\ p)$ where $o < x < \frac{p}{2}$ $\ldots\ldots\ldots\ldots\ldots\ldots (2)$

$\therefore$ $x^2 + 1 = hp$ $\ldots\ldots\ldots\ldots\ldots\ldots (3)$ for some h. Also, $hp = x^2 + 1 < \frac{p^2}{4} + 1 < p^2$

Hence $O < h < p$ $\ldots\ldots\ldots\ldots\ldots\ldots (4)$

(3), (2) and (4) above prove the theorem.

Theorem:

Every prime p of the form $4q+1$ is representable as the sum of two squares.

Proof:

By the well known theorem that there exists a multiple of $'p'$ say $'hp'$ which is representable such that $o < h < p$. If $h = 1$ then there is nothing more to prove. We therefore assume that $h > 1$. Fermat's method of descent consists in proving from this assumption that a smaller multiple of $'p'$ than $'hp'$ is also representable. Let $hp = x^2 + y^2, o < h < p$ for some integers $'x'$ and $'y'$ $\ldots\ldots\ldots\ldots\ldots\ldots$ (1)

This implies $x^2 + y^2 \equiv o \ (mod\ h)$ $\ldots\ldots\ldots\ldots\ldots\ldots$ (2)

If $'r'$ and $'s'$ are the minimal residues of $'x'$ and $'y'$ respectively $(mod\ h)$ then we have $r^2 + s^2 \equiv o\ (mod\ h)$ $\ldots\ldots\ldots\ldots\ldots\ldots$ (3)

Such that $|r| \leq \frac{h}{2}$, $|s| \leq \frac{h}{2}$ It should be noted here that r and s cannot both be zero at the same time, otherwise it would imply that h/x and h/y so that $h^2/x^2 + y^2$ This means that $'h'$ divides $'p'$ which is impossible. From (3) we have $r^2 + s^2 = h_1 h$ $\ldots\ldots\ldots\ldots\ldots\ldots$ (4)

It follows that $h_1 h \leq \left(h/2\right)^2 + \left(h/2\right)^2 < h^2$. Hence $o < h_1 < h$ $\ldots\ldots\ldots\ldots\ldots\ldots$ (5)

From (1) and (2) we obtain $h_1 h^2 p = (r^2 + s^2)(x^2 + y^2)$

$= (rx + sy)^2 + (ry - sx)^2$ $\ldots\ldots\ldots\ldots\ldots\ldots$ (6)

But,

$$rx \equiv x^2\ (mod\ h)$$
$$sy \equiv y^2\ (mod\ h)$$
$$ry \equiv xy\ (mod\ h)$$
$$sx \equiv xy\ (mod\ h)$$

So, $rx + sy \equiv x^2 + y^2 \equiv 0\ (mod\ h)$

Which implies $rx + sy = x_1 h$ $\ldots\ldots\ldots\ldots\ldots\ldots$ (7) for some x_1 Similarly $ry - sx \equiv 0\ (mod\ h)$ (or) $ry - sx = y_1 h$ $\ldots\ldots\ldots\ldots\ldots\ldots$ (8) for some h_1

Thus (6) is transformed to $h_1 h^2 h = h_1^2 h^2 + h_1^2 h^2$ (ie) $h_1 h = h_1^2 + h_1^2,\ 0 < h_1 < h.$

So it is proved that a multiple of *'h'* smaller than *'hh'* is representable. Applying the same process as above to h_1h we get a still smaller multiple of *'h'*, say h_2h, which is representable. Obviously then if we continue the process further we shall finally arrive at result that *'h'* is representable.

Theorem:

Let *'h'* be an odd prime, and let $(h, h) = 1$. Then there exist at least one pair of non zero integers *'h'* and *'h'* each numerically less than $\sqrt{p}$ such that $ua \equiv v \ (mod\ p)$

Proof:

Let $[\sqrt{p}\ ] = h$ so that $h < \sqrt{p} < h + 1$. Consider the integers of the set 's' defined by

$$s = \{sa + t,\ \ s = 1, 2, \dots \dots h + 1;\ \ t = 1, 2, \dots \dots h + 1\}$$

The number of integers in 's' is $(h + 1)^2$ which is greater than 'p' there are at least two integers in 's' which are congruent $(mod\ p)$. Let these be $s_1a + t_1$ and $s_2a + t_2$ where either s_1 is different from s_2 (or) t_1 is different from t_2.

So, we have $s_1a + t_1 \equiv s_2a + t_2 \ (mod\ p) \dots \dots \dots \dots \dots \dots$ (1)

Let us put $s_2 - s_1 = u$ and $t_1 - t_2 = v$. Then $ua \equiv v \ (mod\ p) \dots (2)$

Now if $s_1 \neq s_2$ then $t_1 \neq t_2$ from (1) above

Converse Part:

If $t_1 \neq t_2$ then $s_1 \neq s_2$So in either case 'u' and 'v' are non zero integers. Moreover s_1, s_2, t_1, t_2 are all positive integers which do not exceed $h + 1$.

Hence, $|u| \leq h < \sqrt{p} \dots \dots \dots \dots \dots \dots$ (3)

$|v| \leq h < \sqrt{p} \dots \dots \dots \dots \dots \dots$ (4)

(2), (3) and (4) above establish the theorem.

Theorem:

Every prime of the form $4q + 1$ is representable as the sum of two squares.

Proof:

Since 'p' is of the form $4q + 1, -1$ is a quadratic residue of 'p'. Hence there exist is an integer 'a' which satisfies the congruence. $a^2 + 1 \equiv 0 \ (mod\ p) \dots (1)$ Where $(a, p) = 1$. By the theorem there exist two integers 'u' and 'v' each numerically less than $\sqrt{p}$ such that $ua \equiv v \ (mod\ p)$ (or) $u^2a^2 \equiv v^2 \ (mod\ p)$

But from (1) we have $u^2a^2 + u^2 \equiv 0 \ (mod\ p)$

$$\therefore \quad u^2 + v^2 \equiv 0 \ (mod\ p)$$

This implies $u^2 + v^2 = kp$ for some positive integer 'k'. We know however, that $u^2 + v^2 < 2p$ because $|u| < \sqrt{p}$ and $|v| < \sqrt{p}$

It follows that $u^2 + v^2 = p$.

Theorem:

Let the canonical decomposition of N be $N = 2^h\, p_1^{a_1}\, p_2^{a_2} \dots \dots p_k^{a_k}$ Then N is representable as the sum of two relatively prime squares if and only if $h = 0$ (or) 1 and are primes of the form $4q + 1$.

Proof:

Necessary Part:

Given: $h = 0$ (or) 1 and $p_1, p_2, \dots \dots p_k$ are primes of the form $4q + 1$. To prove that: N is representable as the sum of two relatively prime squares. We know that, -1 is a quadratic residue of $2, p_1, p_2, \dots \dots p_k$ By the well known theorem, "Let $m = 2^h\, p_1^{a_1}\, p_2^{a_2} \dots \dots p_k^{a_k}$. Then '$a$' is a quadratic residue of 'm' if and only if it is a quadratic residue of $2^h, p_1, p_2, \dots \dots p_k$" That -1 is a quadratic residue of N. Therefore there exists an integer 'b', such that $b^2 + 1$ is divisible by N. This implies that N is representable as the sum of two relatively prime squares.

Sufficient Part:

Given: N is representable as the sum of two relatively prime squares. To prove that: $h = 0$ (or) 1 and $p_1, p_2, \dots \dots p_k$ are primes of the form $4q + 1$. Let $N = x^2 + y^2$, $(x, y) = 1$. Then there exists an integer 'b' such that N divides $b^2 + 1$. So -1 is a quadratic residue of N. By the well known theorem, "Let $m = 2^h\ p_1^{a_1}\ p_2^{a_2} \dots \dots p_k^{a_k}$. Then '$a$' is a quadratic residue of 'm' if and only if it is a quadratic residue of $2^h, p_1, p_2, \dots \dots p_k$" That -1 is a quadratic residue of $2^h, p_1, p_2, \dots \dots p_k$ This implies $h = 0$ (or) 1 and $p_1, p_2, \dots \dots p_k$ are primes of the form $4q + 1$. Hence the proof.

Gauss Theorem and Sum of Three Squares:

Theorem:

$R(n)$ = number of lattice points in the interior and on the boundary of the circle $x^2 + y^2 = n$ [excluding the lattice points (0,0)]

Proof

$$R(n) = r(1) + r(2) + \cdots + r(n)$$

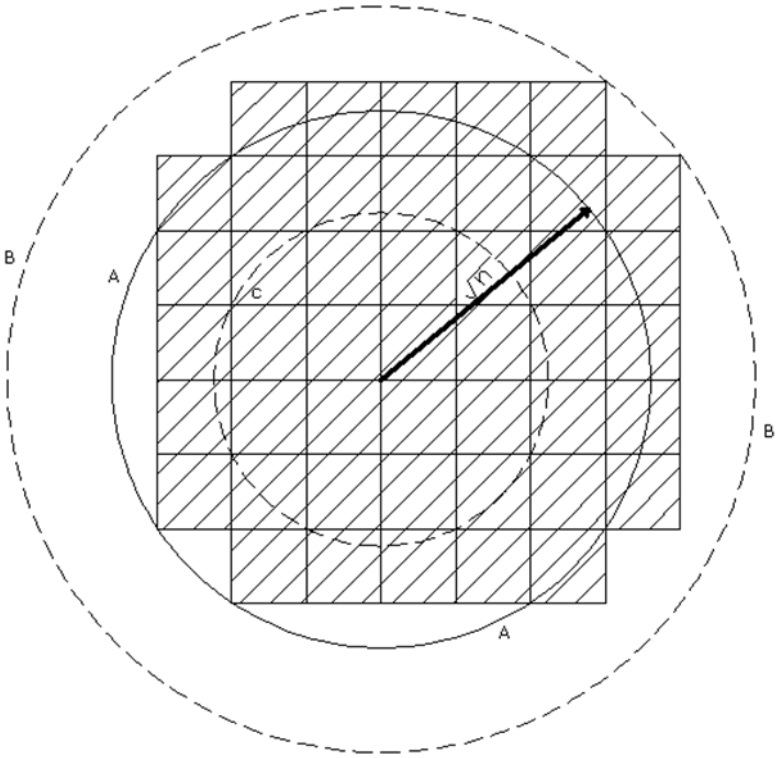
Which is equal to the number of lattice points on the boundaries of the circles $x^2 + y^2 = 1, x^2 + y^2 = 2, \dots \dots \dots, x^2 + y^2 = n$. Hence the proof.

Theorem: (Gauss Theorem)

$$R(n) = \Pi n + o\left(\sqrt{n}\right)$$

Proof:

In the figure, 'A' is the circle $x^2 + y^2 = n$ of radius $\sqrt{n}$.



$R(n) + 1$ is equal to the number of lattice points on and within the circle 'A' including the origin. We attach to each of these $R(n) + 1$ lattice points a lattice square so that lattice points lies at the left hand bottom corner of the square. Then obviously the area of all these squares (shown shaded in the figure) is numerically equal to $R(n) + 1$. Also this area is less than area of the circle 'B' of radius $\sqrt{n} + \sqrt{2}$ and greater than the area of the circle 'C' of radius $\sqrt{n} - \sqrt{2}$.

Hence $\Pi\left(\sqrt{n} - \sqrt{2}\right)^2 < R(n) + 1 < \Pi\left(\sqrt{n} + \sqrt{2}\right)^2$

(or) $\Pi\left(\sqrt{n}-\sqrt{2}\right)^2 - 1 < R(n) < \Pi\left(\sqrt{n}+\sqrt{2}\right)^2 - 1$

But, $\Pi\left(\sqrt{n}+\sqrt{2}\right)^2 - 1 = \Pi n + \left(2\sqrt{2\Pi}\sqrt{n} + 2\Pi - 1\right) = \Pi n + o\left(\sqrt{n}\right)$

Similarly, $\Pi\left(\sqrt{n}-\sqrt{2}\right)^2 - 1 = \Pi n - \left(2\sqrt{2\Pi}\sqrt{n} - 2\Pi + 1\right) = \Pi n + o\left(\sqrt{n}\right)$

It follows that $R(n) = \Pi n + o\left(\sqrt{n}\right)$

Sum of Three Squares:

We shall first consider the representation of an integer as the sum of three squares. We have seen in the last chapter that not all integers can be represented as the sum of two squares. It is therefore natural to inquire whether all integers are representable as the sum of three squares.

For example,

$$4 = 2^2 + 0^2 + 0^2$$
$$5 = 2^2 + 1^2 + 0^2$$
$$6 = 2^2 + 1^2 + 1^2$$

But the integer 7 cannot be so represented. It can only be written as the sum of four squares.

$$7 = 2^2 + 1^2 + 1^2 + 1^2$$

We shall now prove that there are infinitely many integers for which the representation as the sum of three squares is not possible.

Theorem:

If N is of the form $8q + 7$ then N is not representable as the sum of three squares.

Proof:

Let us assume that N is the sum of three squares. $N = x^2 + y^2 + z^2$ for some integers x, y, z. Then it follows that

$$x^2 + y^2 + z^2 \equiv 7 \ (mod\ 8) \ldots\ldots\ldots\ldots\ldots\ldots (1)$$

Now $x^2 \equiv 1 \ (mod\ 8)$ if 'x' odd. $x^2 \equiv 0$ (or) $4 \ (mod\ 8)$ if 'x' even. y^2 and z^2 also be have similarly. Hence $x^2 + y^2 + z^2$ can be congruent $(mod\ 8)$ to one of the integers $0, 1, 2, 3, 4, 5, 6$, and not to 7. Since this contradicts (1) above N cannot br represented as the sum of three squares.

Theorem:

Let $N = 4^h(8q + 7)$ for some 'h' and 'q'. Then N cannot be represented as the sum of three squares.

Proof:

Case (i) Let $h = 0$

Then $N = 8q + 7$ an "By the theorem (2.3)" N is not the sum of three squares.

Case (ii) Let $h \geq 1$

Then if possible let $N = x^2 + y^2 + z^2 \ldots\ldots\ldots\ldots\ldots\ldots$ (1) for some integers x, y, z.

Hence, $x^2 + y^2 + z^2 \equiv 0 \ (mod\ 4) \ldots\ldots\ldots\ldots\ldots\ldots (2)$

Now, $x^2 \equiv 1 \ (mod\ 4)$ if 'x' odd. $x^2 \equiv 0 \ (mod\ 4)$ if 'x' even. It follows that from (2) that x, y, z are all even integers.

$$\therefore \text{ From (1) we have } \left(x/2\right)^2 + \left(y/2\right)^2 + \left(z/2\right)^2 = \left(N/4\right) = 4^{h-1}(8q + 7)$$

It is thus proved that if $4^h(8q + 7)$ is the sum of three squares then $4^{h-1}(8q + 7)$ is also so representable. Repeating the argument in succession we see that, $4^{h-2}(8q + 7, 4h-38q+7, \ldots\ldots\ldots, 408q+7$ are also representable. But we know "by that $408q+7$ is not representable as the sum of three squares. Thus there is contradiction. It follows that N is not the sum of three squares. Conversely, It is possible to prove that if a number N cannot be represented as the sum of three squares then N is of the form $4^h(8q + 7)$.

Sum of Four Squares:

We proved in the previous chapter that it is not possible to represent all numbers as the sum of two squares. The following algebraic identity was first discovered by Euler and it is an essential step towards the solution of the problem.

Result:

$$(x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) = u_1^2 + u_2^2 + u_3^2 + u_4^2$$

Where $u_1 = x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4$

$u_2 = x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3$

$u_3 = x_1y_3 - x_3y_1 + x_4y_2 - x_2y_4$

$u_4 = x_1y_4 - x_4y_1 + x_2y_3 + x_3y_2$

Theorem: (Euler Theorem)

Let 'p' be an odd prime. Then there exist integers x, y, h such that $x^2 + y^2 + 1 = hp$, where $0 \le x < \frac{p}{2}$, $0 \le y < \frac{p}{2}$ and $0 < h < p$.

Proof:

Consider the following two sets of integers $S_1 = \left\{0, 1^2, 2^2, \dots\dots, \left(\frac{p-1}{2}\right)^2\right\}$

$S_2 = \left\{-1, -1 - 1^2, -1 - 2^2, \dots\dots, -1 - \left(\frac{p-1}{2}\right)^2\right\}$

We know that, the integers $1^2, 2^2, \dots\dots, \left(\frac{p-1}{2}\right)^2$ are all incongruent $(mod\ p)$. It follows that the integers of $S_1$and the integers of S_2 also are incongruent $(mod\ p)$. Now, the total number of integers in $S_1 \cup S_2$ is $p + 1$. Therefore there must be at least two integers in these $p + 1$ numbers which are congruent to each other $(mod\ p)$. It then follows that at least one number of S_1, say x^2, is congruent $(mod\ p)$ to some number say $-1 - y^2$ of S_2 such that $0 \le x < \frac{p}{2}$ and $0 \le y < \frac{p}{2}$ Thus we have $x^2 \equiv -1 - y^2\ (mod\ p)$ (or) $x^2 + y^2 + 1 = hp$ for some positive integer 'h'. Further, $h = \frac{1}{p}(x^2 + y^2 + 1) < \frac{1}{p}\left(\frac{p^2}{4} + \frac{p^2}{4} + 1\right) < p$. The theorem is therefore completely proved.

Corollary:

Let 'p' be an odd prime. Then there exists a multiple of 'p' say $ph, 0 < h < p$ which is representable as the sum of four squares.

Proof:

This is easy since by last theorem there exist integers x, y and h. Such that, $x^2 + y^2 + 1^2 + 0^2 = hp$ where $0 < h < p$

Theorem:

Let $'p'$ be any prime. If hp is representable as the sum of four squares for some even integer $'h'$, then $^1/_2\, hp$ is also representable.

Proof:

Let $hp = x_1^2 + x_2^2 + x_3^2 + x_4^2 \dots\dots\dots\dots\dots\dots$ (1)

Then there are five cases with regard to x_1, x_2, x_3 and x_4 which we have to consider (i) They are all even. (ii) One is odd, and the other three even. In this case $(hp = x_1^2 + x_2^2 + x_3^2 + x_4^2)$ would be an odd integer contradicting the given condition. Therefore this case is not possible. (iii) Two of them say x_1 and x_2 are odd and the other two even. (iv) Three are odd and one even. This case is also not possible for the same reasons as in (ii) above. (v) All are odd. Thus cases (i) (iii) and (v) are the only possible ones. In all these three cases it is easily seen that $\frac{x_1 \pm x_2}{2}$ and $\frac{x_3 \pm x_4}{2}$ are integers. The theorem then follows immediately since (1) can be written

$$1/2\ hp = \left(\frac{x_1+x_2}{2}\right)^2 + \left(\frac{x_1-x_2}{2}\right)^2 + \left(\frac{x_3+x_4}{2}\right)^2 + \left(\frac{x_3-x_4}{2}\right)^2$$

Theorem:

Let 'p' be an odd prime. If hp is representable as the sum of four squares for some odd integer $h > 1$ then there exists a smaller multiple of 'p' than hp which is also representable.

Proof:

Let $hp = x_1^2 + x_2^2 + x_3^2 + x_4^2$ ... ... (1) for some integers x_1, x_2, x_3 and x_4

Then obviously $x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv 0\ (mod\ h)$ ... ... (2)

Let the minimal residues of $x_1, x_2, x_3, x_4\ (mod\ h)$ be r_1, r_2, r_3, r_4 respectively. This implies $|r_1| < \frac{h}{2}, |r_2| < \frac{h}{2}, |r_3| < \frac{h}{2}, |r_4| < \frac{h}{2}$

Since 'h' is odd, and $r_1^2 + r_2^2 + r_3^2 + r_4^2 \equiv 0\ (mod\ h)$ ... ... (3)

It should be observed here that r_1, r_2, r_3, r_4 cannot all be simultaneously zero, otherwise it follows that 'h' divides x_1, x_2, x_3, x_4 so that h^2 divides $x_1^2 + x_2^2 + x_3^2 + x_4^2$ (or) that h^2 divides hp which is impossible. From (3) we then have $r_1^2 + r_2^2 + r_3^2 + r_4^2 = h_1 h$ ... ... (4) for some integer h_1

It follows that $h_1 h < \left(h/2\right)^2 + \left(h/2\right)^2 + \left(h/2\right)^2 + \left(h/2\right)^2 = h^2$

So, $h_1 < h$ ... ... (5)

Moreover we obtain from (1) and (4) $h_1 h^2 p = (r_1^2 + r_2^2 + r_3^2 + r_4^2)(x_1^2 + x_2^2 + x_3^2 + x_4^2)$

$= u_1^2 + u_2^2 + u_3^2 + u_4^2$ ... ... (6)

Where by the "Euler Result"

$u_1 = x_1 r_1 + x_2 r_2 + x_3 r_3 + x_4 r_4 \equiv r_1^2 + r_2^2 + r_3^2 + r_4^2\ (mod\ h) \equiv 0\ (mod\ h)$

$u_2 = x_1 r_2 - x_2 r_1 + x_3 r_4 - x_4 r_3 \equiv r_1 r_2 - r_2 r_1 + r_3 r_4 - r_4 r_3\ (mod\ h) \equiv 0\ (mod\ h)$

It can be proved in a similar manner that $u_3 \equiv 0\ (mod\ h)$ & $u_4 \equiv 0\ (mod\ h)$

So, we have $u_1 = s_1 h, u_2 = s_2 h, u_3 = s_3 h$ and $u_4 = s_4 h$ for some integers s_1, s_2, s_3 and s_4

It follows from (6) that $h_1 h^2 p = s_1^2 h^2 + s_2^2 h^2 + s_3^2 h^2 + s_4^2 h^2 = h^2(s_1^2 + s_2^2 + s_3^2 + s_4^2)$

Hence $h_1 p = s_1^2 + s_2^2 + s_3^2 + s_4^2$ ... ... (7)

(7) and (5) prove the theorem.

Theorem:

Every prime 'p' is representable as the sum of four squares.

Proof:

(i) Let $p = 2$ Then $2 = 1^2 + 1^2 + 0^2 + 0^2$ So, 2 is representable.

(ii) Let $p \geq 3$ Then by the corollary. We know that there exists a multiple of 'p' which is the sum of four squares. It follows that there is a least such multiple. Let this be hp. If 'h' is even then by the theorem (3.2) $\frac{1}{2}hp$ is representable. This contradicts our assumption that hp is the least multiple of 'p' which is representable. Therefore 'h' is odd. If, now 'h' is an odd integer > 1, then by the well known theorem, there exists a smaller multiple of 'p' then hp which is representable. This also contradicts our assumption. Hence $h = 1$ and 'p' is representable.

Conclusion:

In this dissertation, we discussed about how an integer can be (or) cannot be represented as a sums of squares. Also, an introduction to number theory and some definitions are discussed. Basic concepts which are used in our dissertation are also discussed. Also, how a number can be (or) cannot be represented as a sum of two squares, sum of three squares and sum of four squares are discussed. These are all the field of current research in Number Theory. So this can be considered as a first step towards my research.

References:

1. Apostol, Tom M. (1976). Introduction to analytic number theory. Undergraduate Texts in Mathematics. Springer. ISBN 978-0-387-90163-3.
2. Apostol, Tom M. (n.d.). "An Introduction to the Theory of Numbers". (Review of Hardy & Wright.) Mathematical Reviews (Math Sci Net) MR0568909. American Mathematical Society. Retrieved 2016-02-28.
3. Boyer, Carl Benjamin; Merzbach, Uta C. (1991) [1968]. A History of Mathematics (2nd ed.). New York: Wiley. ISBN 978-0-471-54397-8
4. Clark, Walter Eugene (trans.) (1930). The Āryabhaṭīya of Āryabhaṭa: An ancient Indian work on Mathematics and Astronomy. University of Chicago Press. Retrieved 2016-02-28.
5. Colebrooke, Henry Thomas (1817). Algebra, with Arithmetic and Mensuration, from the Sanscrit of Brahmegupta and Bháscara. London: J. Murray. Retrieved 2016-02-28.
6. Davenport, Harold; Montgomery, Hugh L. (2000). Multiplicative Number Theory. Graduate texts in mathematics. 74 (revised 3rd ed.). Springer. ISBN 978-0-387-95097-6.
7. Edwards, Harold M. (November 1983). "Euler and Quadratic Reciprocity". Mathematics Magazine. Mathematical Association of America. 56 (5): 285–291. doi:10.2307/2690368.JSTOR 2690368.
8. Edwards, Harold M. (2000) [1977]. Fermat's Last Theorem: a Genetic Introduction to Algebraic Number Theory. Graduate Texts in Mathematics. 50 (reprint of 1977 ed.). Springer Verlag. ISBN 978-0-387-95002-0.
9. Fermat, Pierre de (1679). Varia Opera Mathematica (in French and Latin). Toulouse: Joannis Pech. Retrieved 2016-02-28.
10. Friberg, Jöran (August 1981). "Methods and Traditions of Babylonian Mathematics: Plimpton 322, Pythagorean Triples and the Babylonian Triangle Parameter Equations". Historia Mathematica. Elsevier. 8 (3): 277–318. doi:10.1016/0315-0860(81)90069-0.
11. Fritz, Kurt (2004). "The Discovery of Incommensurability by Hippasus of Metapontum". In Christianidis, J. Classics in the History of Greek Mathematics. Berlin: Kluwer (Springer). ISBN 978-1-4020-0081-2.
12. Gauss, Carl Friedrich; Waterhouse, William C. (trans.) (1966) [1801]. Disquisitiones Arithmeticae. Springer. ISBN 978-0-387-96254-2.
13. Goldfeld, Dorian M. (2003). "Elementary Proof of the Prime Number Theorem: a Historical Perspective" (PDF). Retrieved 2016-02-28.
14. Goldstein, Catherine; Schappacher, Norbert (2007). "A book in search of a discipline". In Goldstein, C.; Schappacher, N.; Schwermer, Joachim. The Shaping of Arithmetic after Gauss' "Disquisitiones Arithmeticae". Berlin & Heidelberg: Springer. pp. 3–66. ISBN 978-3-540-20441-1. Retrieved 2016-02-28.