THE COMPRISE OF GAUSS THEOREM AND SUM OF THREE SQUARES

$Dr.D.R.Kirubaharan^{*}$ and $R.Ramya^{**}$
*Assistant Professor in Mahematics,
PRIST Deemed University
Vallam.Thanjavur − 613403
**Research Scholars
Department of Mathematics
PRIST Deemed University
Vallam.Thanjavur − 613403

Abstract:

Number theory is one of the oldest branches of mathematics and one of the foremost important of course; it concerns questions on numbers, usually meaning whole numbers or rational numbers. Divisibility of integers is a fundamental concept in number theory. Congruence, including Fermat's Little theorem and Euler's theorem extending it, the division "algorithm", the Euclidean algorithm, elementary properties of primes, and the division "algorithm". But the term "elementary" is typically utilized in this setting only to mean that no advanced tools from other areas are used… not that the results themselves are simple.

INTRODUCTION

Number theory, conjointly mentioned as higher arithmetic may even be a branch of arithmetic involved with the properties of integers, rational numbers, irrational numbers and real numbers. Generally the discipline is taken under consideration to include fanciful the delicate numbers conjointly.

Formally, numbers area unit delineate in terms of f sets; there area unit varied schemes for doing this. However, there area unit different ways in which to represent numbers. As angles, as points on a line, as on a plane or as points in house.

The integers and rational numbers area unit usually symbolized and utterly outlined by numerals. The system of numeration normally used these days was developed from utilized in Arab texts; though some students believe they were 1st utilized in Bharat. The questionable Arabic numerals area unit zero, 1, 2,3,4,5,6,7,8 and 9

Indeed, a course in "elementary" variety theory sometimes includes classic and elegant results like Quadratic Reciprocity; investigating results victimization the August Ferdinand Mobius Inversion Formula; and even the prime theorem, declarative the approximate density of primes among the integers, that has tough however "elementary" proofs.

In such chapter we have a tendency to shall discuss the topic of representing positive integers as add of squares of 2 or a lot of integers.

PRELIMINARES

Integers

The numbers $0, 1, -1, 2, -2, 3, -3$ ... are called integers of which $1, 2, 3, ...$ are called positive integers and $-1, -2, -3, ...$ are called negative integers.

The collection of all integers is denoted by Z.

Thus $Z = \{..., -3, -2, -1, 0, 1, 2, 3, ...\}$

Natural Numbers

The numbers $1, 2, 3, ...$ 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 $N = \{ 1, 2, 3, ... \}$

Least Common Multiple

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

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 $b_1, b_2, \dots, b_n$ not all zero by $(b_1, b_2, \dots, b_n)$

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.

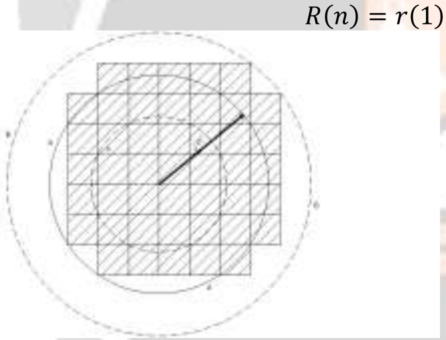
GAUSS THEOREM

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

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

Proof

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

Then by theorem (2.1)

$R(n) + 1$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

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

(or)

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

But,

$$\Pi(\sqrt{n} + \sqrt{2})^2 - 1 = \Pi n + (2\sqrt{2\Pi}\sqrt{n} + 2\Pi - 1)$$

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

Similarly

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

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

Example

$$R(13) = r(1) + r(2) + \cdots + r(13)$$
$$= 4 + 4 + 0 + 4 + 8 + 0 + 0 + 4 + 4 + 8 + 0 + 0 + 8$$

$= 44 = 13\Pi + \theta(\sqrt{13})$ where $|\theta| < 1$

Observe here that θ is positive for $n = 13$.

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

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

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.

∴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, $4^{h-2}(8q + 7), 4^{h-3}(8q + 7), \ldots\ldots\ldots, 4^0(8q + 7)$ are also representable.

But we know
"By the theorem (2.3)"

That$4^0(8q + 7)$ 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$4^h(8q + 7)$.

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) Number Theory – S.G.Telang
2) Number Theory – G.E.Andrews
3) Elementry Number Theory – David M.Burto