RIEMANN AND DIOPHANTINE'S CONTRIBUTION IN THE FIELD OF NUMBER THEORY

[1]Pratik Kumar, [2]Vikas Kumar,
[3]Md Saad Ahmed,[4]Rajnish Tiwari & [5]Md Saquib

[1,2]*Department of Computer Science Engineering*
Institute of Engineering & Management
EP Block, Sector V, Salt Lake, Kolkata-700091. India

[3,5]*Department of Electronic and Communication Engineering*
Institute of Engineering & Management
EP Block, Sector V, Salt Lake, Kolkata-700091. India

[4]*Department of Mechanical Engineering*
Institute of Engineering & Management
EP Block, Sector V, Salt Lake, Kolkata-700091. India
Corresponding Author Email: pratikkr360@gmail.com

Abstract

There have been several fascinating applications of Number Theory in key cryptography. Key cryptography enables many technologies we take for granted, such as the ability to make secure online transactions. The purpose of this survey paper is to highlight certain important such applications. Prime numbers constitute an interesting and challenging area of research in number theory. Diophantine equations form the central part of number theory. An equation requiring integral solutions is called a Diophantine equation. In the first part of this paper, some major contribution in number theory using prime number theorem is discussed and some of the problems which still remains unsolved are covered. In the second part some of the theorems and functions are also discussed such as Diophantine Equation, Goldbach conjecture,Fermats Theorem, Riemann zeta function and his hypothesis that still remain unproved to this day . The Chinese hypothesis is a special case of Fermat's little theorem. As proved later in the west, the Chinese hypothesis is only half right . From the data of this study we conclude that number theory is used in computer network and applications in cryptography.We came to know about the purpose of Diophantine equation , Square-free natural number,Zeta function,Fermat's theorem and Chinese hypothesis which is a special case for Fermat's theorem.

Keywords: *Chinese hypothesis, Diophentine equation, Fermat's theorem, Goldbach conjecture, square-free natural number.*

INTRODUCTION

Number theory is essentially a study of mathematical interaction and number type.There are different types of numbers- odds, evens, squares, integers etc. What number theory does is take these different types of numbers and ask questions about relationship and use formal mathematical proofs to answer questions. One of major tenets of number theory is fundamental theorem of arithmetic that says "all numbers can be factored into a unique set of primes. Earlier it was believed it would be beneficial for math loving people but in 21st century number theory and especially fundamental theorem of arithmetic is being used for encryption schemes for large scale business in computer network. A lot of times a business in computer network is being encrypted using prime factorization. Unique prime factorization of huge numbers is the key to business network. It has applications in cryptography and many other areas of mathematics. The prime factorization of integers is a central point of study in number theory and number theorists study prime numbers as well as the properties of objects made out of integers(for example ,rational numbers) or defined as generalization of the integers (for example, algebraic integers).German mathematician Carl Friedrich Gauss said,"Mathematics is the queen of the sciences- and number theory is the queen of mathematics."There are three basic tools which are often used in proving properties of integers.They are :the well ordering principle ,the principle of mathematical induction .With help of Euclidean algorithm ,greatest common divisor of two integers can be found out.One major contribution in number theory was prime number theorem.It was known that there were infinitely many primes and there are arbitrary large gaps between primes.But we were not able to estimate how many primes are there less than a given number?This theorem solved this problem which was estimated by Chebyshev and proved by Hadamard and Poussin.This theorem states that there is no need to find all the primes less than x to find out their number ,it will be enough to evaluate x/log(x) for large x to find an estimate for the number of primes.Euler's totient function counts the number of positive integers less than a given integer that are relatively prime to that given integer.In other words,it is the number of integers k in the range 1=<k=<n for which is the greatest common divisor gcd(n,k) is equal to 1.The integers k of this form are sometimes referred as totatives of n.For example, the totatives of n=9 are the six numbers 1,2,4,5,7,8.They are all relatively prime to 9,but other three numbers in this range 3,6 & 9 are not, because gcd(9,3)=gcd(9,6)= 3 and gcd(9,9)=1.

Some Unsolved Questions:

Some of the problems of number theory which still remain unsolved are:

1. Are there infinitely many primes given by the polynomial $f(x)=x^2+1$?
2. Is there always a prime between x^2 and $(x+1)^2$?
3. Do any odd perfect numbers exist?
4. Are there infinitely many primes of the form $n^2 + 1$ (i.e., one more than a perfect square)?

5.Are there infinitely many pairs of twin primes (i.e., primes that differ by 2, like 5 and 7 or 41 and 43)?
6.Is Goldbach's conjecture true? (Euler failed to prove it; so has everyone since.)
Goldbach conjecture, in number theory is that every even counting number greater than 2 is equal to the sum of two prime numbers. More precisely, Goldbach claimed that "every number greater than 2 is an aggregate of three prime numbers."

METHODOLOGY

The distribution of primes is a fascinating area of research.Euclid devoted part of his Elements to prime numbers and divisibility, topics that belong unambiguously to number theory and are basic to it . In particular, he gave an algorithm for computing the greatest common divisor of two numbers and the first known proof of the infinitude of primes .Working with lengths, areas, & volumes, it's theorized that the GCD algorithm was of great importance to Euclid because it provided a way to *find the largest common length between any two segments a and b.*Euler proved Fermat's little theorem but was not able to solve every problem. He gave proofs, or near-proofs, of Fermat's last theorem for exponents n = 3 and n = 4 but despaired of finding a general solution. And he was completely stumped by Goldbach's assertion that any even number greater than 2 can be written as the sum of two primes. Euler endorsed the result—today known as the Goldbach conjecture—but acknowledged his inability to prove it.Ernst Kummer went further, demonstrating that Fermat's last theorem was true for a large class of exponents; unfortunately, he could not rule out the possibility that it was false for a large class of exponents, so the problem remained unresolved.The theory of numbers, is a vast and challenging subject as old as mathematics and as fresh as today's news. Its problems retain their fascination because of an apparent simplicity and an irresistible beauty. With such a rich and colourful history, number theory surely deserves to be called, in the famous words of Gauss, "the queen of mathematics."

ANALYSIS

Riemann zeta function: $f(x)=1 + 2^{-x} + 3^{-x} + 4^{-x} +\ldots$ Riemann zeta function is a special function of mathematics that arises in definite integration and related with result surrounding theorem many of the property of this function have been investigated, their remain important fundamental hypothesis (Riemann hypothesis) that remain unproved to this day .Riemann extended the study of the zeta function to include the complex numbers $x= iy$, where $i = \sqrt{-1}$, except for the line x=1 in the complex plane. Riemann knew that the zeta function equals zero for all negative even integers -2, -4, -6,…-9. So called trivial zeros and that it has an infinite numbers of zeros in the critical strip of complex numbers that fall strictly between the lines x=0 and x=1. He also knew that all nontrivial zeros are symmetric with respect to the critical line x=1/2. Riemann conjectured that all of the nontrivial zeroes are on the critical line , a conjecture that subsequently became

known as the Riemann hypothesis.The Riemann zeta function satisfy the reflection functional equation which is:$f(1-s) = 2(2\pi)^{-s}\cos(1/2*s*\pi)\ \Gamma(s)f(s)$

A linear diophentine equation is of the form ax+by=c.The purpose of Diophantine equation is to solve for all the unknown in the problems. When Diophantine was dealing with 2 or more unknowns in terms of only one of them these equations can fall into two catogries: (A) determine equations of different degrees or (B) indeterminate equations . Determine equations are divided into pure determinate equations, mixed quadratic equations simultaneously equations involving quadratic and cubic equations. Pure equation are those that contain only one power of the unknown, whatever the degree. Quadratic equations contain unknowns with degree powers of 2 and 1. Diophantus only dealt with one particular case in arithmetic concerning cubic equations.Diophantine equations are equations of polynomial expressions for which rational or integer solution are sought. Usually, the term implies that we want integer solutions, but in a sense these are equivalent. If a given equations has rational solutions, a corresponding equation with integer solutions can be found by multiplying the first equation by an integer constant, namely, the least common multiple of the denominators of the numbers obtained by raising the solutions to the appropriate power . As the name suggests, many problems that we now call diophantus equations are addressed in the arithmetic of diophantus. However, some of these problems were known well before the time of diophantus also, some of the most famous problems of number theory , such as fermai's last theorem, are Diophantine equations posed by mathematicians living much later.Two well-known results from beginning number theory are example of Diophantine equations which predict diophantus. These are linear equations of two variables, that is ax + by = c, and the quadratic equations of three variables,$x^2 + y^2 = z^2$. Both of these problems were known by the Babylonians. Solutions to the second are often known as pythagorean triangles, or Pythagorean triples, since a geometric interpretation of this is length of the sides of a right triangle, and the expression is, of course, the Pythagorean theorem. Fermat's last theorem, that $x^n + y^n = z^n$ has no solution for n>2, is a generalization of this.

Fermats theorm:Fermat's theorem, also known as fermat's primality test, in number theory, the statement, first given by French mathematician Pierre de fermat, that for any prime number p and any integer a such that p does not divide a (the pair are relatively prime), p divides exactly into a^p-a . although a number n that does not divide exactly into a^n- a for some 'a' must be a composite number, the converse is not necessarily true. For example, let a = 2 and n = 341, then a and n are relatively prime and 341 divides exactly into 2^{341}-2 however, 341= 11x31, so it is a composite number (a special type of composite number known as a pseudoprime). Thus, fermat's theorem gives a test that is necessary but not sufficient for primality. As with many of fermat's theorems, no proof by him is known to exist. A special case of fermat's theorem, known as the chinese hypothesis which replaces a with 2, states that a number n is prime if and only if it divides exactly into $2^n - 2$. As proved later in the west, the chinese hypothesis is only half right. Chinese hypothesis:A prime p always satisfies the condition that 2^p-2 is divisible by p. however, this

condition is not true exclusively for prime (e.g., $2^{341} - 2$ is divisible by 341 = 11x31). Composite numbers n (such as 341) for which $2^n - 2$ is divisible by n are called poulet numbers, and are a special class of fermat pseudoprimes. The chinise hypothesis is a special case of fermat's little theorem.

Square-Free Natural Number:A natural number n is said to be square-free if it is not divisible by the square of a number > 1.Therefore n is square-free if and only if it is the product of distinct primes.An interesting problem is to determine the probability that a given natural number n is square-free.Gauss observed that the probability that two integers should be relatively prime is $(6/\pi^2)$. The probability that a number should be square-free is $(6/\pi^2)$.

CONCLUSION

Following the completion of our research paper on number theory we conclude that number theory is used in various purpose like computer network and business network using prime factorization and applications in cryptography.Know about the problems faced like about the existence of odd perfect numbers, occurrence of infinitely many pairs in the form of $n^2 + 1$ and about goldbach's conjecture.Perhaps we conclude that goldbach's conjecture remains a challenge in the near future.We learnt about the Riemann zeta function which are generally used in definite integration. Also came to know about the purpose of Diophantine equation which is to solve for the unknowns in the problems.Learnt about Fermat's theorem which is also known as Fermat's primality test and this theorem was given by French mathematician Pierre de Fermat. Learnt about the Chinese hypothesis which is a special case for Fermat's theorem which states that a prime p always satisfies the condition that $2^p - 2$ is divisible by p.

REFERENCES

1.Number theory available at www.britanica.com/science/number-theory/prime-number-theorem#referenceto33908

2. Wissam Raji.An Introductory course in elementary number theory

Available at www.resources.seller.org/wwwresources/archived/site/wp-content/uploads/2013/05/An-Introductory-in-Elementry-Number-Theory.pdf

3. Application of number theory available at. www.researchgate.net/publication/269806702 Applications of Number Theory in Statistics

4.Plato, *Theaetetus*, p. 147 B, (for example, Jowett 1871), cited in von Fritz 2004, p. 212: "Theodorus was writing out for us something about roots, such as the roots of three or five, showing that they are incommensurable by the unit;...".