IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2320-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 10, Issue 6, June 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.512

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|(A High Impact Factor, Monthly, Peer Reviewed Journal)

|| Volume 10, Issue 6, June 2021 ||

| DOI:10.15680/IJIRSET.2021.1006445|

Number Theory in Maths

Dr. Manish Kumar Sareen

Associate Professor, Department of Mathematics, SNDB Govt. PG College, Nohar, Hanumangarh, India

ABSTRACT: Number theory is the study of the integers (e.g. whole numbers) and related objects. Topics studied by number theorists include the problem of determining the distribution of prime numbers within the integers and the structure and number of solutions of systems of polynomial equations with integer coefficients.

KEYWORDS: number theory, integers, prime, polynomial, coefficients

I. INTRODUCTION

Unsurprisingly, number theorists are interested in the properties of numbers! In particular, the relations between the additive and multiplicative structures of integers are so fascinating that they make number theory a vast and fertile field of mathematical research. Gauss, who is often known as the 'prince of mathematics', called mathematics the 'queen of the sciences' and considered number theory the 'queen of mathematics'.[1,2,3]

Many problems in number theory can be formulated in a relatively simple language. For example, the famous last theorem of Fermat states that there exists no non-trivial integer solution of the equation $x^n + y^n = z^n$ for $n \geq 3$. The twin prime conjecture is to ask if there should be infinitely many primes p such that p+2 is also a prime. Although these questions are easily stated, they are so deep that they have withstood attempts to prove them for centuries. Fermat's last theorem was only proved in 1995 by A. Wiles after the cumulative effort of many mathematicians for more than 350 years, while the twin prime conjecture remains open even today.

The great difficulty in proving relatively simple results in number theory prompts many new concepts in mathematics. Over the centuries, this discipline has grown very much with close connections to other areas of mathematics: algebraic geometry, representation theory, combinatorics, cryptography and coding theory, probability, harmonic analysis and complex analysis.

The Pure Mathematics department teaches number theory courses at various levels. The elementary number theory course is offered twice per year. The analytic number theory and the algebraic number theory course are available every other year. We also teach advanced topic courses on a regular basis. Major areas of interest for number theorists in the Pure Mathematics department include Diophantine equations and Diophantine approximation, arithmetic geometry, L-functions and random matrix theory, representation theory, computational number theory, and additive and probabilistic number theory.

Number Theory is the branch of mathematics that deals with the study of positive numbers and arithmetic operations based on them. Numbers are the mathematical entities that are used for counting. Since the development of human civilization, numbers have always been a source of fascination for various mathematicians across the globe.

Discrete mathematics deals with counting individual items, such as whole numbers, rather than continuous quantities like real numbers. Number theory, a major component of discrete math, delves into the properties and behaviors of integers, especially natural numbers and occasionally all integers.

Understanding number theory is crucial in comprehending fundamental concepts in discrete math, as it provides insights into divisibility, prime numbers, modular arithmetic, and other key areas of study.

The definition of number theory states that it is a branch of pure mathematics devoted to the study of natural numbers and integers. It is the study of the set of positive whole numbers usually called the set of natural numbers. This theory is experimental and theoretical. While the experimental number theory leads to questions and suggests different ways to answer them, the theoretical number theory tries to provide a definite answer by solving it. Theoretically, numbers are classified into different types, such as natural numbers, whole numbers, complex numbers, and so on. Observe the following figure which shows the relationship between whole numbers, integers, and rational numbers.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|(A High Impact Factor, Monthly, Peer Reviewed Journal)

|| Volume 10, Issue 6, June 2021 ||

| DOI:10.15680/IJIRSET.2021.1006445|

Number Theory Sub-classification
The numbers which are used in our day-to-day life can be classified into different categories. Here is a list that shows the subclassification of numbers:

Odd Numbers
Odd numbers are those that are not divisible by the number 2. Numbers like 1, 3, 5, 7, 9, 11, 13, 15, and so on are considered as odd numbers. On the number line, 1 is considered as the first positive odd number.

Even Numbers
Even numbers are integers that are divisible by the number 2. For example, 2, 4, 6, 8, 10, 12, 14, 16, and so on are even numbers.

Square Numbers
Numbers that are multiplied by themselves are called square numbers or perfect square numbers. For example, in $3 \times 3 = 9$, 9 is a square number. Similarly, 1, 4, 9, 16, and so on are square numbers.

Cube Numbers
Numbers that are multiplied by themselves 3 times are called cube numbers. For example, 27 is a cube number because $3 \times 3 \times 3 = 27$. Similarly, 1, 8, 64 are cube numbers.

Prime Numbers
Prime numbers are numbers that have only 2 factors, 1 and the number itself. For example, 3 is a prime number because it has only two factors, 1 and 3. In the same way, 2, 5, 7, 11 are prime numbers.

Composite Numbers
Unlike prime numbers that have only 2 factors, composite numbers are those that have more than 2 factors. In other words, composite numbers can be divisible by more than two numbers. For example, 6 is a composite number because it has more than two factors, that is, it is divisible by 1, 2, 3, and 6.[4,5,6]

Fibonacci Numbers
A series of numbers where a number is the addition of the last two numbers, starting with 0 and 1 is known as the Fibonacci sequence. The numbers in this series or sequence are known as Fibonacci numbers. For example, 0, 1, 1, 2, 3, 5, 8, 13, 21, 34, ..., is the Fibonacci sequence. Here, we can see that $1 + 1 = 2$, $1 + 2 = 3$, $2 + 3 = 5$, $3 + 5 = 8$ and so on.

Number Theory Uses
Number theory is used to find out if a given integer 'm' is divisible with the integer 'n' and this is used in many divisibility tests. This theory is not only used in Mathematics, but also applied in cryptography, device authentication, websites for e-commerce, coding, security systems, and many more.

II. DISCUSSION

Number theory is the study of properties of the integers. Because of the fundamental nature of the integers in mathematics, and the fundamental nature of mathematics in science, the famous mathematician and physicist Gauss wrote:

"Mathematics is the queen of the sciences, and number theory is the queen of mathematics."
There are an abundance of simply formulated questions about the integers that involve little more than the basics of addition and multiplication (the ring operations on the integers), but which are nevertheless unsolved or extremely difficult to solve. For example:
•Which integers can be written as the sum of four squares?
•If $n \geq 3 n \geq 3$ is a positive integer, can a positive $n$thnth power ever be written as the sum of two positive $n$thnth powers?
•Is there a rectangular box whose side lengths, face diagonal lengths, and body diagonal length are all integers?

The first question was solved long ago by Lagrange: every nonnegative integer can be written in this way.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|(A High Impact Factor, Monthly, Peer Reviewed Journal)

|| Volume 10, Issue 6, June 2021 ||

| DOI:10.15680/IJIRSET.2021.1006445|

The second question is due to the 17th17th-century mathematician Fermat, who famously claimed in 1637 to have discovered a proof that the answer is no. Though the answer is no, this was not rigorously established until 1995, when Andrew Wiles completed a difficult and sophisticated proof that built on the work of dozens of leading contemporary mathematicians. The result is popularly known as Fermat's last theorem.

The third question is one of many number-theoretic questions whose answer is currently unknown. It is possible to produce infinitely many boxes (sometimes called Euler bricks) for which all the sides and face diagonals are integers, but no one has been able to construct such a box with integer body diagonal length as well, or to prove that no such box exists.

Divisibility

The first nontrivial facts about the integers relate to the concept of divisibility: if a,a,b are two integers, then $b|a$b|a (read "bb divides aa") if and only if there is an integer cc such that $bc=a$.bc=a.

The integers have a division algorithm, where two integers can be divided with remainder: for any $a,\in Z$a,b∈Z with $b\neq 0$,b⌊=0, there is a unique integer qq and a unique integer rr with $0\leq r<|b|$0≤r<|b| satisfying $a=bq+r$.a=bq+r. Here qq is the quotient and rr is the remainder.

In the division algorithm, if $d|a$d|a and $d|b$,d|b, then $d|r$.d|r. So iterating the division algorithm gives a way to compute the greatest common divisor of aa and b,b, called the Euclidean algorithm. The greatest common divisor also satisfies Bezout's identity--the integers of the form $ax+by$ax+by are precisely the multiples of the greatest common divisor of aa and b,b, and in particular, the gcd⨍₀gcd itself can be written as $ax+by$ax+by for some integers x,y.x,y. In fact, possible values of xx and yy can be computed using the extended Euclidean algorithm.

These computations and algorithms are useful in various applications of elementary number theory; see below for examples.

Prime Numbers

Main article: Prime numbers

Let aa be a positive integer. If bb is a divisor of aa that is not equal to 11 or aa (i.e. bb is a nontrivial proper divisor of aa), then aa can be factored as $a=bc$,a=bc, where bb and cc are nontrivial proper divisors of a.a. Then we can break down bb and cc similarly to get an expression for aa as a product of smaller divisors.

The process stops only when each of the divisors in the product cannot be broken down further; in other words, when the divisors in the product do not have any nontrivial proper divisors.

If a=12,a=12, then b=2b=2 is a nontrivial proper divisor. So 12=2·6.12=2·6. Now 22 has no nontrivial proper divisors, but 66 does: 2|6,2|6, so 6=2·36=2·3 and 12=2·2·3.12=2·2·3.

Integers greater than 11 with no nontrivial proper divisors are called prime numbers.[7,8,9]

The above discussion shows that every integer can be decomposed as a product of prime numbers. So the prime numbers are the multiplicative building blocks of the integers. This fact is so important that it is known as the fundamental theorem of arithmetic:

Every positive integer can be written as a product of prime numbers. The factorization is unique up to rearrangement of the factors.

The distribution of primes inside the integers is a difficult and rich topic of research. There are infinitely many primes, a fact which was known to Euclid. A much more sophisticated estimate is the prime number theorem, which says roughly that the probability of a random integer $\leq x\leq$x being prime is about 1ln⨍₀x.lnx1. Other, more precise estimates often involve the Riemann hypothesis, a deep and unsolved conjecture about the zeroes of a certain complex-valued function.

Still other elementary questions about the prime numbers remain open. In particular, the twin prime conjecture that there are infinitely many prime numbers pp such that $p+2$p+2 is also prime, and the Goldbach conjecture that any even integer $\geq 4\geq$4 can be written as a sum of two primes, are still unsolved despite centuries of efforts by countless mathematicians.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|(A High Impact Factor, Monthly, Peer Reviewed Journal)

|| Volume 10, Issue 6, June 2021 ||

| DOI:10.15680/IJIRSET.2021.1006445|

Modular Arithmetic

Results involving divisibility are often most easily stated using modular arithmetic. If two integers aa and bb leave the same remainder when divided by an integer n,n, we write $a \equiv b \pmod{n}$,a≡b(modn), read "aa is congruent to bb mod n.n." For example, 64≡1(mod7),64≡1(mod7), or −1007≡3(mod10).−1007≡3(mod10).

Basic rules of modular arithmetic help explain various divisibility tests learned in elementary school. For instance, Every positive integer is congruent (mod3)(mod3) to the sum of its digits.
Forexample, 268=100·2+10·6+1·8268=100·2+10·6+1·8 iscongruent
to 1·2+1·6+1·8,1·2+1·6+1·8, because 100,10,100,10, and 11 are all congruent to 11 mod 3.3. This holds for any power of 10:10: $10^k \equiv 1^k \equiv 1 \pmod{3}$,10k≡1k≡1(mod3), so the statement is true no matter how many digits the integer has.

The operations of addition, subtraction, and multiplication work as expected, but there is also a form of division. In particular, the equation $x \equiv 1/(\mathrm{mod} n)$x≡1/a(modn) makes sense if $ax \equiv 1 \pmod{n}$.ax≡1(modn). Such an xx exists if and only if gcd(a,n)=1,gcd(a,n)=1, by Bezout's identity.

The set {0,1,…,n−1}{0,1,…,n−1} of representatives of integers mod n,n, with operations given by modular addition and modular multiplication, is often called Zn.Zn. The subset of ZnZn consisting of invertible elements is called $Zn*$Zn∗; it is closed under multiplication and has $\varphi(n)$φ(n) elements, where φφ is Euler's totient function. In particular, when pp is prime, $Zp*$Zp∗ consists of all the elements of ZpZp except 0,0, so it has $p-1$p−1 elements.

This is the setup for one of the first nontrivial theorems of elementary number theory, known as Fermat's little theorem. If pp is prime and $p \nmid a$,pł a, then $a^{p-1} \equiv 1 \pmod{p}$.ap−1≡1(modp).
This generalizes to any modulus nn:
Euler's theorem: If gcd(a,n)=1,gcd(a,n)=1, then $a^{\varphi(n)} \equiv 1 \pmod{n}$.aφ(n)≡1(modn).
These theorems have a myriad of diverse applications to, for instance, primality testing, periods of decimal expansions of fractions, and modern cryptography. Some examples of the latter will be outlined in the following section.

Applications to Cryptography

Some basic problems in elementary number theory are well-suited for use in modern cryptography. Many cryptosystems require a computationally difficult one-way process, which is quick to do but hard to reverse. The two most common such processes both come from number theory.

One such process is factoring: it is easy for a computer to multiply two large prime numbers together, but very difficult to recover the prime numbers given their product.[10,11,12] If $N=pq$N=pq where p,qp,q are large prime numbers, finding pp and qq is equivalent in difficulty to finding $\varphi(N)=pq-p-q+1$.φ(N)=pq−p−q+1. This fact, coupled with Euler's theorem, is the foundation of the widely-used RSA cryptosystem.

Another such process is the so-called discrete log problem: given coprime integers aa and nn (where nn is taken to be very large), and an integer k,k, it is easy to compute $a^k \pmod{n}$,ak(modn), but it is difficult to recover kk given a,n,a,n, and $a^k \pmod{n}$.ak(modn). This idea is the foundation of the Diffie-Hellman protocol.
More recently, these ideas have been extended and enriched by replacing modular arithmetic by the more exotic operations on points on elliptic curves.

Diophantine Equations

Many of the oldest questions in number theory involve what are now known as Diophantine equations: polynomial equations in multiple variables with integer coefficients, where the unknowns are constrained to be integers as well. Indeed, the problem of finding the solutions to the simplest linear Diophantine equation, $ax+by=c$,ax+by=c, is essentially the content of Bezout's identity.

Very simple Diophantine equations often have very difficult solutions. The techniques involved often come from other areas of mathematics, most notably algebraic geometry: the solutions to a Diophantine equation can be viewed as special points (points with integer coordinates) on a larger geometric object like a curve or surface, cut out by the real or complex solutions to the same equation.

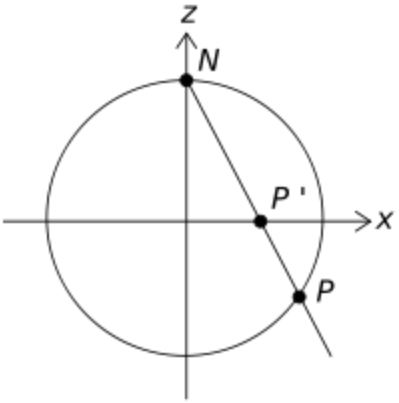
For example, the positive integer solutions to Pythagoras's equation $x2+y2=z2$,x2+y2=z2, known as Pythagorean triples, were of interest more than 2500 years ago. Dividing through by $z2$z2 gives $(x/z)2+(y/z)2=1$,(x/z)2+(y/z)2=1, so

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|(A High Impact Factor, Monthly, Peer Reviewed Journal)

|| Volume 10, Issue 6, June 2021 ||

| DOI:10.15680/IJIRSET.2021.1006445|

a Pythagorean triple corresponds to a point $(x/z,y/z)$(x/z,y/z) with rational coordinates on the circle $X2+Y2=1$.X2+Y2=1. One way to parameterize all such points is via the geometric trick of starting with a rational point on the circle (say (0,1)(0,1)), drawing a line with rational slope through it, and looking for the other point of intersection, which is guaranteed to be rational. Parameterizing Pythagorean triples.[1]



Generalizations of Pythagoras's equation abound, but the degree of difficulty rises quickly. In particular, increasing the exponent leads to a famously difficult theorem:
Fermat's last theorem: The equation $xn+yn=zn$xn+yn=zn has no solutions in positive integers x,,x,y,z for any integer value of $n\geq 3$.n≥3.
Restricting attention to sums of squares leads to fundamental classical results about which integers can be expressed as sums of two, three, and four squares; in particular, every positive integer is the sum of four squares. Asking about sums of higher powers leads to an even deeper set of results known collectively as Waring's problem.

On the other hand, the Euler brick question in the introduction gives an example of a specific system of Diophantine equations whose solutions have not yet been determined. There is even a general negative result known as Hilbert's tenth problem that states that there can be no universal algorithm for determining whether any Diophantine equation has a solution. Current research in this area tends to center on specific types of Diophantine equations which are of particular interest to mathematicians for some reason (elliptic curves are an especially fertile subject), but there are still many unsolved problems along these lines.

Algebraic Number Theory
Main article: Algebraic number theory
Here is a problem that can be solved using properties of rings other than the integers. (The preliminary analysis uses modular arithmetic in a common way as well.)

Find all integer solutions to $y2=x3-1$.y2=x3−1.

_____

Here is a proof sketch.
First note that if xx is even, then $y2\equiv 3 (\mathrm{mod} 4)$,y2≡3(mod4), which is impossible, so xx is odd and thus yy is even. Rewrite as $y2+1=x3$y2+1=x3 and factor$(y+i)(y-i)=x3$.(y+i)(y−i)=x3.Any common factor of $y+i$y+i and $y-i$y−i must be a common factor of their difference $2i=(1+i)2$.2i=(1+i)2. [13,14,15]It is not hard to check that $1+i$1+i is prime, in the following sense: its only divisors are the units (divisors of 1) $\pm 1,\pm i$±1,±i and unit multiples of itself. But if $1+i$1+i divides $y+i$,y+i, say $(1+i)(c+di)=y+i$,(1+i)(c+di)=y+i, we get $y=c-d$y=c−d and $1=c+d$,1=c+d, which would imply that yy was odd, which is impossible.
So $y+i$y+i and $y-i$y−i are relatively prime. Two numbers that are relatively prime whose product is a cube must both be cubes themselves. But $y+i=(a+bi)3$y+i=(a+bi)3 gives $y=a3-3ab2$y=a3−3ab2 and $1=3a2b-b3=b(3a2-b2)$.1=3a2b−b3=b(3a2−b2). This only works if bb and $3a2-b2$3a2−b2 are both $\pm 1,\pm 1$, which is only possible if $b=-1$b=−1 and $a=0$.a=0. This leads to $y=0,=1$,y=0,x=1, which is the only solution.

The proof sketch above can be made rigorous, but there are some holes in the proof as written--in particular, the first two sentences of the last paragraph assume that the Gaussian integers, the complex numbers of the form $a+bi$a+bi where a,ba,b are integers, have similar properties to the integers themselves. In particular, there needs

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|(A High Impact Factor, Monthly, Peer Reviewed Journal)

|| Volume 10, Issue 6, June 2021 ||

| DOI:10.15680/IJIRSET.2021.1006445|

to be a well-defined sense of "relatively prime" and an analogue of the fundamental theorem of arithmetic in the ring [i]Z[i] of Gaussian integers.

While the ring [i]Z[i] does have the properties required to make the above proof rigorous--most notably, a form of unique factorization into irreducible elements--other, similar rings do not have the same properties.

In the ring [−5],Z[−5], factorization into irreducible elements is not necessarily unique. For example,6=2·3=(1+−5)(1−−5)6=2·3=(1+−5)(1−−5)and each of the four factors is irreducible (its only factors are ±± itself or 1).

Incorrect assumptions about rings of this type led to false starts at proofs of Fermat's last theorem in the 19th century. The theory of such rings is beautiful and interesting on its own, but it also has many applications to down-to-earth questions about the integers. Here are a few examples:

- as in the example above, for many specific Diophantine equations, finding solutions and showing that a given solution set is complete by using arithmetic in a ring larger than the integers
- proofs of Fermat's two-square theorem (using the Gaussian integers) and Lagrange's four-square theorem (using quaternions)
- a deeper understanding of quadratic reciprocity and generalizations of it to higher reciprocity laws
- primality testing (via e.g. the Lucas-Lehmer primality test) and factorization algorithms (via e.g. the number field sieve)

Analytic Number Theory

The use of complex analysis to solve difficult number-theoretic problems has a rich history, dating back nearly 200 years to the French mathematician Dirichlet. The original motivating problem was the prime number theorem, which gives an effective asymptotic estimate for the number $\pi(x)$π(x) of primes $\leq x$.≤x. Dirichlet himself used complex-analytic tools to prove his famous theorem on the density of primes in arithmetic progressions: he showed that for coprime positive integers aa and n,n, there are infinitely many primes congruent to aa mod n,n, but his actual result was much stronger--of the $\varphi(n)$φ(n) possible congruence classes for a prime mod n,n, Dirichlet showed that the primes were (asymptotically) distributed equally among those classes.

The techniques of analytic number theory can often be described in the following general way:

- Create a complex-valued function related to number-theoretic objects of interest, such as prime numbers or sums of powers;
- Use tools of complex analysis (e.g. line integration, the residue theorem, analytic/meromorphic continuation) to gain analytic information about the function;
- Develop correspondences between analytic properties of the function and the original number-theoretic objects;
- Translate the analytic information to results (often, asymptotic estimates) of the number-theoretic objects one wishes to study.

A classical example of this technique involves the Riemann zeta function$(s)=\sum n=1\infty 1ns,\zeta(s)=n=1\sum\infty ns1$,where ss is a complex number whose real part is larger than 1.1. Expressing $(s)\zeta(s)$ as a certain integral allows it to be extended (or "continued") to a function defined everywhere on the complex plane with the exception of a simple pole at s=1.s=1.

The relationship to the prime numbers comes via the Euler product representation$(s)=\prod p$ prime$11-p-s.\zeta(s)=p$ prime$\prod$ 1−p−s1.Famously, facts about the values of ss for which $\zeta(s)=0\zeta(s)=0$ correspond to deep facts about the distribution of prime numbers. There are "trivial" zeroes at s=−2,−4,…,s=−2,−4,…, but it is immediate from the form of the analytic continuation that the other zeroes must all lie in the strip $0\leq Re(s)\leq 1.0\leq Re(s)\leq 1$. The Prime Number Theorem turns out to be equivalent to the statement that there are no zeroes on the edge of the strip, the line Re(s)=1.Re(s)=1.[16,17,18]

In fact, computational evidence suggests that all the zeroes lie in the center of the strip, Re(s)=1/2;Re(s)=1/2; and this is the famous Riemann hypothesis. It is still unsolved, and it is of great interest precisely because it implies many interesting facts about the distribution of primes, including an improvement on the accuracy of the estimate given in the Prime Number Theorem.

Generalizations of the zeta function called Dirichlet series can be used to study other arithmetic functions as well.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|(A High Impact Factor, Monthly, Peer Reviewed Journal)

|| Volume 10, Issue 6, June 2021 ||

| DOI:10.15680/IJIRSET.2021.1006445|

Another famous result proved using analytic techniques (due to Hardy and Littlewood) was an explicit estimate of the number of powers involved in Waring's problem:

(Vinogradov) Let kk be a positive integer. Every positive integer can be written as a sum of $G(k)$G(k) nonnegative $k$kth powers, where $G(k) \leq 3k\log(k)+11k$.G(k)≤3klog(k)+11k.

III. RESULTS

In which years does February have five Sundays? How many right-angled triangles with whole-number sides have a side of length 29? How many shuffles are needed to restore the order of the cards in a pack with two Jokers? Are any of the numbers 11, 111, 1111, 11111, . . . perfect squares? Can one construct a regular polygon with 100 sides if measuring is forbidden? How do prime numbers help to keep our credit cards secure?

These are all questions in number theory, the branch of mathematics that's primarily concerned with our counting numbers, 1, 2, 3, etc. Of particular importance are the prime numbers, the 'building blocks' of our number system.

The subject is an old one, dating back to the ancient Greeks, and for many years has been studied for its intrinsic beauty and elegance, not least because several of its challenges are so easy to state that everyone can understand them, and yet no-one has ever been able to resolve them.

This lecture situates the above problems and puzzles in their historical context, drawing on the work of many of the greatest mathematicians of the past, such as Euclid, Fermat, Euler and Gauss. Indeed, as Gauss, sometimes described as the 'Prince of Mathematics', has claimed: Mathematics is the Queen of the Sciences, and Number Theory is the Queen of Mathematics.

The integers and prime numbers have fascinated people since ancient times. Recently, the field has seen huge advances. The resolution of Fermat's Last Theorem by Wiles in 1995 touched off a flurry of related activity that continues unabated to the present, such as the recent solution by Khare and Wintenberger of Serre's conjecture on the relationship between mod p Galois representations and modular forms. The Riemann hypothesis, a Clay Millennium Problem, is a part of analytic number theory, which employs analytic methods (calculus and complex analysis) to understand the integers. Recent advances in this area include the Green-Tao proof that prime numbers occur in arbitrarily long arithmetic progressions. The Langlands Program is a broad series of conjectures that connect number theory with representation theory. Number theory has applications in computer science due to connections with cryptography.

The research interests of our group include Galois representations, Shimura varieties, automorphic forms, lattices, algorithmic aspects, rational points on varieties, and the arithmetic of K3 surfaces.
Anyone who has ever fallen in love will tell you it's the little things about the other person that matter. The silly in-jokes shared at the end of the day. The peculiarities of the other person's morning coffee ritual. The way he or she lets old paperbacks stack up on the bedside table. Such interrelated details come to define us. They trace the undercurrents of our personality, and, to the observant and loving eye, they illuminate true beauty.

In the eyes of some, there is no finer beauty than that found in mathematics. They look at the world of numbers and, just as you'd never define your human beloved solely by his or her profession or hair color, the math lover sees beyond the mere function of numbers. The likes of 6, 28 and 496 turn into something more sublime than simple carriers of information. Independent of their usage, numbers become fascinating entities, and their mathematical relationships express the complexity of a vast system underpinning nature itself.

The study of those sometimes subtle and far-reaching relationships is number theory, sometimes referred to as higher arithmetic. Number theorists scrutinize the properties of integers, the natural numbers you know as -1, -2, 0, 1, 2 and so forth. It's part theoretical and part experimental, as mathematicians seek to discover fascinating and even unexpected mathematical interactions.

What kind of relationships? Well, we actually categorize integers into different number types based on their relationships. There are, of course, odd numbers (1,3, 5 …), which cannot be divided evenly, and even numbers (2, 4, 6 …), which can. There are square numbers, produced by multiplying another number by itself. For instance, 2 x 2 = 4

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|(A High Impact Factor, Monthly, Peer Reviewed Journal)

|| Volume 10, Issue 6, June 2021 ||

| DOI:10.15680/IJIRSET.2021.1006445|

and 3 x 3 = 9, so 4 and 9 are both square numbers. So is 1 (1 x 1 = 1) and so is 9,801 (99 x 99 = 9,801). We also express these four examples as 22, 32, 12 and 992.

Now let's add another level of intrigue to this example. In some cases, we can add square numbers together to produce other squared numbers in what is called a Pythagorean triple, as they fit the Pythagorean theorem (a2 + b2 = c2). An example of this is 32 + 42 = 52, or 3, 4, 5.[19]

IV. CONCLUSION

So, the world of math offers up numerous number types, each with its own particular properties. Mathematicians formulate theories about the relationships between numbers and number groups. They uphold their theories with axioms (previously established statements presumed to be true) and theorems (statements based on other theorems or axioms).

The first step in building a shiny, new, mathematical theory, however, is asking a theoretical question about number relationships. For example, can the sum of two cubes be a cube? Remember the Pythagorean triples from the previous page? These trios of three numbers, such as (3, 4, 5), solve the equation a2 + b2 = c2. But what about a3 + b3 = c3? Mathematician Pierre de Fermat asked the same question about cubes and, in 1637, he claimed to have worked out a mathematical proof that, via line after line of painstaking logic, showed beyond any doubt that no, the sum of two cubes can't be a cube. We call this Fermat's Last Theorem. Unfortunately, instead of providing the full proof in his notes, Fermat merely wrote, "I have a truly marvelous demonstration of this proposition which this margin is too narrow to contain" [source: NOVA].

More than three and a half centuries followed during which mathematicians around the world tried in vain to rediscover Fermat's proof. What was riding on this quest? Nothing, save academic pride and the love of pure, abstract mathematics. Then in 1993, with the aid of computational math undiscovered in Fermat's time, English mathematician Andrew Wiles succeeded in proving the 356-year-old theorem. Experts continue to dispute whether Fermat actually worked out such a phenomenal proof in his pre-computer age, or if he was mistaken.

Other questions in number theory related to various perceived or theoretical patterns in numbers or number groups. It all begins with that most crucial aspect of intelligent thought: pattern recognition. Brown University mathematics professor Joseph H. Silverman lays out five basic steps in number theory:

Accumulate mathematical or abstract data.
Examine the data and search for patterns or relationships.
Formulate a conjecture (typically in the form of an equation) to explain these patterns or relationships.
Test the conjecture with additional data.
Devise a proof showing the conjecture to be correct. The proof should start with known facts and end with the desired result.

Fermat's Last Theorem, therefore, was really a conjecture for 356 years and only became a true theorem in 1993. Others, such as Euclid's Proof of Infinite Primes (which proves that prime numbers are limitless), has remained a solid model of mathematical reasoning since 300 B.C. Still other number theory conjectures, both old and new, remain unproofed.
Numbers are as infinite as human understanding is finite, so number theory and its various subfields will continue to captivate the minds of math lovers for ages. Old problems may fall, but new and more complicated conjectures will rise.

Emerging Applications
For the most part, number theory remains a purely abstract area of mathematical study, but applications do exist in the field of cryptography, where number theory can create simple yet highly secure codes. Other fields of application include digital information processing, computing, acoustics and crystallography.[20]

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|(A High Impact Factor, Monthly, Peer Reviewed Journal)

|| Volume 10, Issue 6, June 2021 ||

| DOI:10.15680/IJIRSET.2021.1006445|

REFERENCES

1. Long 1972, p. 1.
2. ^ Neugebauer & Sachs 1945, p. 40. The term takiltum is problematic. Robson prefers the rendering "The holding-square of the diagonal from which 1 is torn out, so that the short side comes up...".Robson 2001, p. 192
3. ^ Robson 2001, p. 189. Other sources give the modern formula . Van der Waerden gives both the modern formula and what amounts to the form preferred by Robson.(van der Waerden 1961, p. 79)
4. ^ van der Waerden 1961, p. 184.
5. ^ Neugebauer (Neugebauer 1969, pp. 36–40) discusses the table in detail and mentions in passing Euclid's method in modern notation (Neugebauer 1969, p. 39).
6. ^ Friberg 1981, p. 302.
7. ^ van der Waerden 1961, p. 43.
8. ^ Iamblichus, Life of Pythagoras,(trans., for example, Guthrie 1987) cited in van der Waerden 1961, p. 108. See also Porphyry, Life of Pythagoras, paragraph 6, in Guthrie 1987 Van der Waerden (van der Waerden 1961, pp. 87–90) sustains the view that Thales knew Babylonian mathematics.
9. ^ Herodotus (II. 81) and Isocrates (Busiris 28), cited in: Huffman 2011. On Thales, see Eudemus ap. Proclus, 65.7, (for example, Morrow 1992, p. 52) cited in: O'Grady 2004, p. 1. Proclus was using a work by Eudemus of Rhodes (now lost), the Catalogue of Geometers. See also introduction, Morrow 1992, p. xxx on Proclus's reliability.
10. ^ Becker 1936, p. 533, cited in: van der Waerden 1961, p. 108.
11. ^ Becker 1936.
12. ^ van der Waerden 1961, p. 109.
13. ^ 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;..." See also Spiral of Theodorus.
14. ^ von Fritz 2004.
15. ^ Heath 1921, p. 76.
16. ^ Sunzi Suanjing, Chapter 3, Problem 26. This can be found in Lam & Ang 2004, pp. 219–220, which contains a full translation of the Suan Ching (based on Qian 1963). See also the discussion in Lam & Ang 2004, pp. 138–140.
17. ^ The date of the text has been narrowed down to 220–420 CE (Yan Dunjie) or 280–473 CE (Wang Ling) through internal evidence (= taxation systems assumed in the text). See Lam & Ang 2004, pp. 27–28.
18. ^ Dauben 2007, p. 310
19. ^ Libbrecht 1973
20. ^ Boyer & Merzbach 1991, p. 82.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.512

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर
NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details