J. of Ramanujan Society of Math. and Math. Sc. **ISSN : 2319-1023**
Vol.6, No.1 (2017), pp. 145-156

SOME RECENT ADVANCES IN NUMBER THEORY

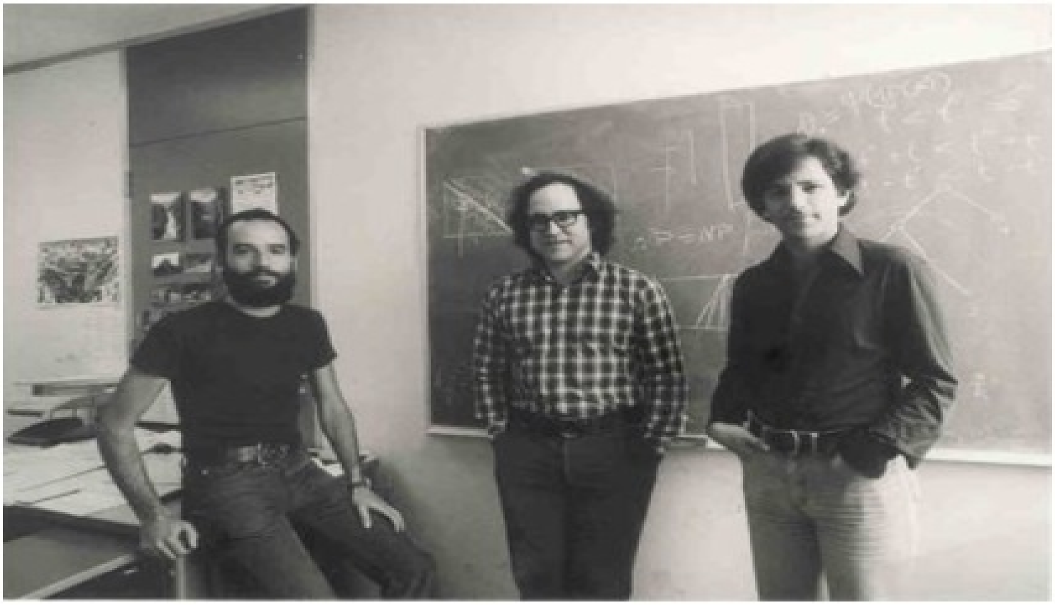
P.V. Arunachalam

Former President, Indian Mathematical Society
E-mail: arunapuduru@gmail.com

Dedicated to Prof. K. Srinivasa Rao on his 75^{th} ***Birth Anniversary***

1.	**RSA Algorithm**	−1977
2.	**Andrew Wiles-FLT**	−1995
3.	**AKS Primality Test**	−2002
4.	**Terence-Tao AP & Primes**	−2006
5.	**Yitang Zhang-"Bounded Gaps"**	−2011

1. RSA Algorithm -1977
(Ron Rivest, Adi Shamir, Leonard Andleman)



Encryption is the standard method for making a communications private. Anyone who wants to send a private message to another user, encrypts (enciphers) the message before transmitting it. Only the intended recipient knows how to correctly decrypt (decipher) the message. Any one who has been "eavesdropping" on the communication could only see the encrypted message. He does not know how to decrypt it successfully. As such privacy can be ensured in electronic communications.

Cryptosystem is a system to encrypt and decrypt information. These are of two kinds: public key or private key.

Private key encryption methods, use the same key to both encrypt and decrypt data. The key must be known only to the parties who are authorized to encrypt and decrypt a particular message.

Public - Key encrypto-systems use different keys to encrypt and decrypt data. The public keys is globally available. The private key is kept confidential.

(1977) The RSA (Rivest - Shamir - Adleman of MIT-US) algorithm is one of the most popular and secure public - key encryption methods. The algorithm capitalizes on the fact has there is no efficient way to factor very large, 100 to 200 digit, numbers.

To use an encryption key (e, n), the algorithm is as follows.

1. Represent the message as an integer between 0 and $(n-1)$. Large messages can be broken up into numbers of blocks. Each block would then be represented by an integer in the same range.

2. Encrypt the message by raising it to the e^{th} power modulo n; the result is the cipher text message. (Cipher text = message in the encrypted form)

3. To decrypt cipher text message C raise to another power d modulo n.

The encryption Key (e, n) is made public. The decryption Key (d, n) is kept private, by the user.
How to determine appropriate values for e, d and n?

1. Choose two very large (100 + digit) prime numbers. Denote these numbers by p and q.

2. Set n equal to $p * q$.

3. Choose any large number d such that $GCD\{d, (p-1) * (q-1)\} = 1$

4. Find e such that $e * d = 1 \bmod (p - -1) * (q - -1)$.

Rivest, Shamir and Adleman provided efficient algorithms for each required operation 4.

Note: The asymmetry in the encryption key which is public and the decryption key which is kept secret, is based on the practical difficulty of factoring the product of two large prime numbers.

A user of RSA creates and then publishes a public key based an two large prime numbers along with an auxiliary value. The prime numbers must be kept secret. Anyone can use the public key to encrypt a message, but with currently published methods, if the public key is large enough, only someone with the knowledge of prime numbers can feasibly decode the message.

Why are primes important in cryptography?

Cryptography is all about numbers theory. All integer numbers, except 0 and 1 are made up of primes. So we deal, a lot with primes in number theory.

RSA critically depend on the fact that prime factorization of large numbers takes a long time.

Basically you have a “public key” consisting of a product of two large primes used to encrypt a message, and a “secret key” consisting of the primes used to decrypt the message. You can make the “public key” public, and every one can use it, to encrypt messages to you, but only you know the prime factors and can decrypt the messages. Every one would have to factor the number, which takes too long to be practical, given the current state of the art of number theory.

Note: Any operation done to data that can only be undone by knowing either of the two factors, will be non-trivial to un-encrypt. Suppose you have a very very large integer which is known to be the product of two primes m and n, it is not easy to faid what are m and n. RSA algorithm exploits this secret. It takes lot of time to factorise. For the hacker, if any algorithm takes lot of time to break the code, it becomes useless.

Note: The whole security of RSA is based on the fact that it is not easy to factorize large composite numbers.

2. Andrew Wiles-FLT -1995

Fermat himself proved it for $n = 3$ & $n = 4$, He also recognized that if a solution existed for any power of n, then it would exist for a multiple of n. We need consider only prime powers.

Ernst Kummer in 1850, proved FLT for special kind of prime numbers, he called regular primes and regular primes maybe defined via some divisibility criteria.

Euler proved FLT independently for $n = 3, n = 4$.

Dirichlet (1805-1859) proved it for $n = 5$ (Legendre 1830)

Lame and Lebesgue in 1840 for $n = 7$

Sophie Germain (1776-1831) worked in this field and made a considerable headway. She proved that if a solution of Fermat's equation with $n = 5$ existed, then all these numbers had to be divisible by 5. This result separated FLT into two cases.

Case 1 for numbers not divisible by 5

Case 2 for numbers that are

The theorem was generalized to other powers, and she gave a general theorem which allowed a proof of FLT for all primes n less than 100 in case 1.

Kummer (1810-1893) came closer than anyone else, to a general solution of Fermats problem. Kummer invented an entire mathematical - theory, the theory of Ideal numbers, in attempting to prove FLT. He proved FLT for all exponents less 100 as well as infinitely many multiples of prime numbers in this range. This was quite an achievement.

Richard Dedekind (1831-1916) abstracted Kummer's Ideal numbers and developed a new theory of Ideals, which inspired Barry Mazur and Mazur's own work was exploited by Andrew Wiles.

Andrew Wiles-Fermat's Last Theorem

Fermat himself was able to prove his theorem for n = 4 as already pointed out. Leading mathematicians at different times proved the result for exponents 3, 5, 6 and 7. But all these were only for particular cases. What was needed was a general proof that would work for all exponents, however large they might be.
Euler (1707-1783), Sophie Germain (1776-1831), Dirichlet (1805-1859), Legendre, Gabriel Lame(1795-1870), Kummer (1810-1893), Cauchy (1789-1857) and many others tried their luck.

In 1922, the English Mathematician LJ. Mordell discussed a very strange connection between the solution of algebraic equation and topology.

Andrew Wiles & Fermat

Elliptic Curves: Diophantine problem of third century began to be studied more and more in the 20^{th} century CE, using elliptic curves. Elliptic curves have nothing to do with ellipses or elliptic functions. $y^2 = ax^3 + bx^2 + cx$ where a, b, c are integers or rational numbers, represents an elliptic curve.

When one looks at the rational points on the elliptic curves, these numbers form a group. Number theorists have become fascinated with the elliptic curves, since they can answer many questions about equations and their solutions. Thus elliptic curves became one of the foremost research tools in number theory. The experts in Number theory knew that some of the elliptic curves they were studying were modular, that is these few elliptic curves could be viewed as connected with the modular forms. To understand a little bit of the idea of modularity, we take the simple circle $x^2 + y^2 = a^2$. Look at the simple periodic function.

$x = a \cos t, y = a \sin t$.

These two functions can stand for x and y in the equation of the circle. The equation of the circle is modular in this same.

A modular elliptic curve is just an extension of this idea to the more complicated complex plane, with a special non Euclidian geometry.
Note: A modular form is a (complex) analytic function on the upper half plane satisfying a certain kind of functional equation with respect to the group action of the modular group, and also satisfying a growth condition. The theory of modular forms therefore belong to complex analysis but the main importance of the theory has traditionally been in its connection with number theory. Andrew Wiles proof of Fermat's last theorem is a proof of the modularity theorem for semi elliptic curves, together with the Ribet's theorem. Both FLT and the modularity theorem were almost universally considered inaccessible to proof by contemporaneous mathematicians and were seen as, virtually impossible to prove using current knowledge.

The present proof itself is over 150 pages long. John Coats described the proof as one of the highest achievements of number theory, and John Conway called it the proof of the century.

2. AKS Primality Test (2002)

AKS Primality Test: It is the Agrawal -Kayal -Saxena primality test and is also known as cyclotomic AKS Test. This is a deterministic primality proving algorithm created and published by Mahindra Agarwal, Neeraj Kayal and Nithi Saxena, Camputer Scientists at IIT Kanpur, on August 6, 2002 in a paper titled "PRIMES is in P". The algorithm determines whether a number is prime or composite within polynomial time. The authors received the 2006 Godel prize and the 2006 Fulkerson prize for this work.

AKS is the first primality proving algorithm to be simultaneously general, polynomial, deterministic and unconditional. Previous algorithms had been developed for centuries and achieved three of those properties at most, but not all four.

AKS Primality Test (2002)

The AKS algorithm can be used to verify the primality of any general number given.

The maximum running time of the algorithm can be expressed as a polynomial over the number of digits in the target number.

The algorithm is guaranteed to distinguish deterministically whether the target number is prime or composite.

The test is based upon the following theorem: An integer $n \geq 2$ is prime if and only if the polynomial congruence relation

$$(x+a)^n \equiv (x^n + a) \mod n \tag{1}$$

holds for some a co-prime to n. This theorem is a generalization to polynomials of Fermat's Little theorem, and can be proven using the binomial theorem, together with the following property of the binomial coefficient.

$\left(\begin{array}{c} n \\ k \end{array} \right) \equiv 0 \pmod{n}$ for all $0 < k < n$ if and only if n is prime.

While relation (1) constitutes a P.T (Primality Test) in itself, Verifying it takes exponential time. Therefore to reduce the computational complexity, AKS makes use of the related congruence.

$$(x+a)^n \equiv (x^n + a) \pmod{(n, x^r - 1)} \tag{2}$$

$$\text{which is same as } (x+a)^n - (x^n + a) = nf + (x^r - 1)g \tag{3}$$

for some polynomials f and g. This congruence can be checked in polynomial time when r is polynomial to the digits of n, because it is provable that r need only be logarithmic with respect to n.

A glance at the of Primality Testing

The Sieve of Eratosthenes

Wilson's characterization

Fermat's primaliry test

Solovay - Strassen primality test

Euclidean Algorithm

In a simpler way we can give the following version of the AKS algorithm for testing whether a number is prime in a polynomial time algorithm based on elementary theorem about Pascal triangles.

The theorem on which the test is based can be stated as follows:

A number p is prime iff all the coefficients of the polynomial expansion of $(x - 1)^p - (x^p - 1)$ are divisible by p. For example try $p = 3$, $(x - 1)^3 - (x^3 - 1) =$

$(x^3 - 3x^2 + 3x - 1) - (x^3 - 1) = -3x^2 + 3x$. All the coefficients are divisible by 3 . So 3 is prime.

4. Terence Tao- (2004)-Green-Tao Theorem

Terence Tao was born in July 1975. He has been a Professor of Mathematics in UCLA, since he was 24. He is an Australian American Mathematician. He works in number of areas of Mathematics; namely

Harmonic Analysis.

PDE

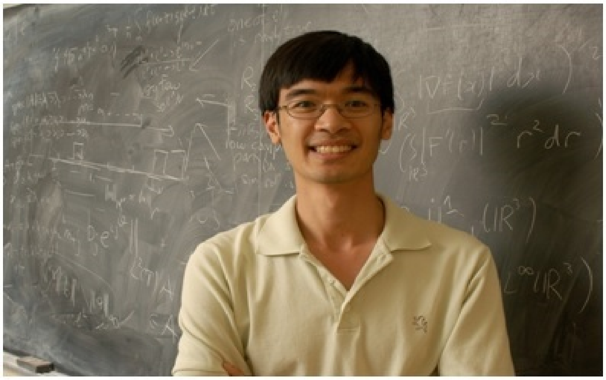
Algebraic Combinatorics

Geometric Combinatorics

Compressed Sensing

Analytic Number Theory

He was a co-recipient of the 2006 Fields Model and Breakthrough prize in Mathematics 2014. Tao exhibited extraordinary Mathematical abilities attending University level math courses since the age of nine. In IMO, he got bronze, silver and gold medals in 1986, 1987 and 1988 respectively. He remains the youngest winner of each of the three medals in the Olympiads' history. He won the gold medal before his 14th birthday. He got his master's degree at the age of 16 (Flinder's University). He won a Fulbright scholarship to pursue P.G. studies in U.S.



He collaborated with Ben. J.Green of Oxford University. Together they proved Green-Tao theorem (2004). This theorem states that there are arbitrarily long arithmetical progressions of primes. The New York Times reported "In 2004, Tao along with Ben Green, a mathematician now at the university of Cambridge, in England, solved a problem related to the Twin Prime Conjecture, by looking at prime number progressions- series of numbers equally placed (For example 3, 7 and 11 constitute a progression of Prime numbers with a spacing of 4, the next in the sequence, 15 is not Prime). Dr Tao and Dr Green proved that it is always possible to find, some where in the infinity of integers, a progression of Prime numbers of equal spacing and any length". For this and other work, Tao was awarded the Australian Mathematical Society Medal 2004. In August 2006, at the 25^{th} ICM in Madrid, he became one of the youngest persons, the first Australian and the first UCLA faculty member ever to be awarded a Fields Medal.

An article by "New Scientist" writes about his ability: "Such is Tao's reputation that mathematicians now compete to interest him in their problem and he is becoming a kind of Mr. Fixit for frustrated researcher. "If you are stuck on a problem, then one way out is to interest Terence Tao" says Charles Fefferman, Prof. of Mathematics at Princeton University.

TAO won the Fields Medal for his contribution to PDE, Combinatorics, Harmonic Analysis and Additive Number Theory. People started to describe him as the Mozart of Mathematics. He is arguably the world's best Mathematician says Joseph Rudnick, Dean of Physical Science, UCLA.
Green-Tao Theorem: The sequence of Prime numbers contains arbitrary long arithmetic progressions. In other words, there exist A.P.'s of Primes, with k terms, where k is any natural number. This theorem does not show how to find the progressions of primes, it merely proves they exist. There has been separate computational work to find large arithmetic progressions in the Primes.

On Jan 18, 2007. Jaroslaw Wroblewski-found the first known case of 24 primes in A.P. $468,395,662,504,823 + (205,619)\ X\ (23\#)X\ n, n = 0, ...23$. Here 23# is a primorial equal to the product $2 \times 3 \times 5... \times 19 \times 23 = 223,092,870$.
On May 17, 2008, Wroblewski and Raanan Chermoni found the first known case of 25 primes $6,171,054,912,832,631 + (366,384) * (223,092,870n), n = 0, ...24$
On April 12, 2010, Benoat Perichon extended this work to 26 terms. $43,142,746,595,714,191 + (23,681,770) * (223,092,870n), n = 0...25$.
We recall the following:

Erdos' conjecture on Arithmetic Progressions.

This is also known as Erdos-Turan Conjecture. It is a Conjecture on arithmetic combinotorics. If the sum of the reciprocals of the members of a set A of positive integers diverges, then A contains arbitrarily long A.P.'s Formally the conjecture states that if $\sum 1/n$ where $n \in A$, diverges then A contains arithmetic progressions of any given length. Set A of this type is called large set.

Dirichlet Theorem on arithmetic progressions: For any tow positive coprime integers a and b there are infinitely many primes of the form a+nb where n is a non- negative integer.

In other words there are infinitely many primes which are congruent to a modulo b.

The numbers of the form $a+nb$ form an arithmetic progression $a, a+b, a+2b, a+3b, ...$ and Dirichlet theorem states that this sequence contains infinitely many prime numbers, if $(a, b) = 1$.

Breakthrough Prize (Physics, Life Sciences and Mathematics):

This award was announced in 2013 by Yan Milner and Mark Zuckerberg. The first awards of the prize worth 3 million dollars to each recipient, were made in 2014.

Terence Tao got this prize for numerous breakthrough contributions to harmonic analysis, combinatorics, PDE's and analytic number theory.

5. Yitang Zhang (2012)-Bounded Gap Between Primes

Yitang Zhang: A Chinese born (1955) American Mathematician working in the area of number theory. He is a professor in the University of New Hampshire US, since 2013. Zhang's problem is often called - "bound gaps". It concerns prime numbers. The question of whether there is a boundary within which, on an infinite number of occasions, two consecutive prime numbers can be found, especially out in the region where the numbers are so large that it would take a book to print a single one of them. Daniel Goldston (U.S.), Jonos Pintz (Budapest), Cem Yildirim

(Istanbul) working together in 2005, had come closer than anyone else to establishing whether there might be a boundary, and what it might be. Zhang devoted himself to bound gaps for a couple of years without finding a door. Once he said, "We could not see any hope." Then on July 3, 2012 in the afternoon, "within five or ten minutes the way is open". Zhang finished "bounded gaps between primes" in the 2012.

After checking thoroughly on April 17, 2013, without talking to any one, he sent the paper to Annals of Mathematics. Editorial Board of Annals is always skeptical of work from some one they have never heard of. In 2013, Annals received 915 papers and accepted 37. The wait between acceptance and publication is typically around a year. The referees of Zhang's paper felt that "the main results are of the first rank. The author has succeeded to prove a land mark theorem in the distribution of prime numbers." They added, "although we studied the arguments very thoroughly, he found it very difficult to spot even a smallest slip. We are very happy to strongly recommended acceptance of the paper for publication in the Annals."

No formula predicts the occurrence of primes. They become as if they appear randomly. As the primes get larger, they grow scarcer and the distances between them, the gaps, grow wider. There are 25 primes between 1 and 100, 168 between 1 and 1000 and 78, 498 between 1 and a million.

"Bounded gaps between primes" is a back door attack on the twin prime conjecture, which was proposed in the nineteenth century and says that no matter how has far you travel on the number line, even as the gap widens between primes, you will always encounter a pair of primes that are separated by two. The twin prime conjecture is still unresolved. Euclid's proof established that there will always be primes, but it says nothing about how far apart any two might be. Zhang established that there is a distance within which, on an infinite number of occasions, there will always be two primes.

Take the line of positive integers marked green if they are composite and red if they are prime. Zhang chose a ruler of a length of 70 million, because a number that large made it easier to prove his conjecture. If he had been able to prove the twin prime conjecture, the number for the ruler world have been two. This ruler can be moved along the line of numbers and enclose two primes an infinite number of times.

From Zhang's result a deduction can be made by using pigeon hole principle that there is a number smaller than seventy million which precisely defines a gap of separating an infinite number of pairs of primes .With in a week of Zhang's announcement, mathematicians around the world began competing to find a lower number. It was Terence Tao who initiated a cooperative project for this propose. The project is called Polymath 8 started in March 2013. Taking advantage of the related work of a young British mathematician, James Maynard, the project reduced the bound to 246.