P: ISSN No. 2231-0045 RNI No. UPBIL/2012/55438 VOL.-III, ISSUE-I, August-2014
E: ISSN No. 2349-9435

Periodic Research

A Visit to the World of Primes

Abhishek Mukheerjee
Assisitant Professor,
Deptt. of Mathematics,
Kalna College,Kalna
The University of Burdwan

Abstract

The theory of numbers has always occupied a unique position in the world of mathematics. but we are dealing with the primes which are very much uncanny in nature. in this article we want look into some special type of primes and their history. we also give a little bit information about the primality tests and the largest prime found so far.

Keywords: Natural, Number, Primes, Mersenne Primes, Product.

Introduction

”Kronecker” once expressed that”**God Created The Natural Numbers And All the Rest Is The Work of Man**”. The naturals played an important role in each and every part of mathematics. one may ask that “why has number theory held such an irresistible appeal for the leading mathematicians?”Answer lies in the basic nature of its problem. When we go to play with the numbers we must face a beautiful type of numbers called” the prime number” which is not being dominated by any formula so far.But as we go through these numbers we will encounter a lot of different types of primes which can be characterized sometimes and sometimes not.In this paper we will take a glimpse of all these things and also discuss about some real life application of the primes which is happening from the middle of twentieth century. Today prime number s has many practical uses and some technical uses also ,but the most prolific work would be to find out the largest one.

History of Numbers

There is a dictum that anyone who want to get at the root of a subject should first go through its history.Endorsingthis,I intend to frame the material into a historical backgrounds throughtout.

The theory of numbers elementarily concerned with the properties of naturals 1,2,3,4,………..,the origin of which hints back to the **Greeks** for whom the number meant positive integer.**Greeks** were largely indebted to the **Babylonians** and ancient **Egyptians** for a extensive study about the naturals.The first rudiments of an actual theory are credited to the **Pythagoras** and **Pythagorians** in between 580B.C.-500B.C.,where they believed that “**Everything Is A Number**”.Their doctrine is a mixture of cosmic philosophy and number mysticism which assigned to everything material and spiritual a definite integer such as 1 represented reason,that could produce only a consistent body of truth;2 stood for man;3 for woman;4 was the Pythagorian symbol of justice,being the first number which is the product of equals;5 identified with marriage,being the product of 2 and 3;and so on.

In 350 B.C. history met with a distinguished mathematician named “***EUCLID***”,founder of **School of Mathematics**,and author of the oldest greek treatise the “**Elements**”which was a compilation of many mathematical inventions available at that time,organized in 13 parts or BOOKS amongst which only three of them ,**VII,VIII,IX**,were devoted to the numbers.It was widely circulated and studied throughout the world,having a thousand of editions since the first printed version in 1482.In the seventh Book of the “Elements” we may trace out a elegant tool to find out g.c.d. of two integers,called the Division Algorithm which is now renamed as the **Euclidean Algorithm**.It is to be noted that the French mathematician **Gabriel Lame**`(1795-1870) proved that the No. of steps required in the Euclidean Algorithm is at most five times the No. digits in smaller integer.

Now it is the right time to enter into the large playground of primes.The first surviving records of extensive study of primes and their characteristics come from the ancient Greek mathematicians around 500 B.C.Now before entering into a vast discussion ,let’s define what are the primes?

Definition

A positive integer p>1 is defined to be a prime if its only positive divisors are 1 and p.An integer >1 which is not a prime ,is called a composite.In 300 B.C.,Euclid proved the Fundamental Theorem of rithmetic and the infinitude of primes which was embodied in IX Book of the Elements, universally regarded as a model of mathematical excellance and elegant.

The Fundamental Theoremo Arithmetic

states that “Every positive integer greater than 1 ,except for the order of factors,be represented as a product of primes in one and only one way”.

This at once kicks you to treat the primes as the building blocks of our number system from which we can generate other integers.Also we have to admit that the Pythagorians deserve the credit of being the first to classify the numbers into even and odd;prime and composite.

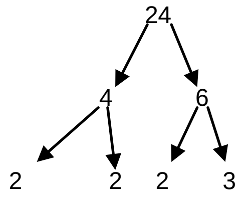


Figure 1.
This is a factor tree that breaks 24 down its prime factors

The interesting fact is that the Alphabets is made up of a finite number of letters that may create an infinite number of words,while there are a finite number of digits that may create infinitely many numbers.Observing these facts we are tempted to pose an obvious query that “are the primes finite in number?” or “do the primes go on forever?”

Again Euclid’s excellancy poured into this and it goes like this “Given any finite list of primes ,one can always find a prime not in the given list” or in a nutshell “There is an infinite number of primes”

Infinitude of Primes (Eucid)

There is an infinite number of primes[1].

Sketch of the Proof

Given a finite list of primes ,say {p1,p2,…………..,pn},consider the number p# =p1.p2……pn +1.Using Fundamental theorem of Arithmetic you can easily show that there exists a prime p such that p/p# **-** p1.p2…..pn i.e. p/1 -a contradiction.

Though Euclid’s actual statement was as follows:

Theorem

Prime numbers are more than any assigned multitude of prime numbers.

Determining Prime Numbers

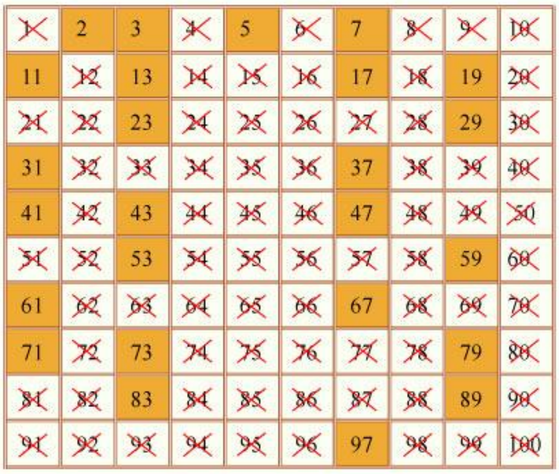
Thanks to Euclid ,since we know that primes are infinite in number,but the question is” Given a particular integer,how can we determine whether it is prime or composite?” How would you pick out the primes amongst the naturals?The story begins now………

After 100 years of Euclid’s discoveries,another Greek mathematician,whose work in number theory remains significant,named “***Erastosthenes of Cyrene***”(276-194B.C.) provided a way of determining what are the primes.

Sieve of Erastosthenes

We can easily check that “if an integer a>1 is not divisible by a prime $p\le\sqrt{a}$,then a is of necessity a prime”.

Erastosthenes used this observation as the basis of a clever technique, called the ”**Sieve of Erastosthenes**” which is basically an algorithm for finding all the primes below a given integer n.The scheme calls for writing down the integers from 2 to n in their natural order and then systematically eliminating all the composite numbers by striking out all multiples 2p,3p,4p,5p,…..of the primes $p\le\sqrt{n}$.The integers that are left in the list – those that do not fall through the “sieve” –are primes.



~~1~~	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~

Figure.2.
This shows the first 100 numbers after the sieve of Erastosthenes has been completed.

We list that **2,3,5,7,11,13,17,19,23,29,31,37,41,43,47,53,59,61,67, 71,73,79,83,89,97** are all the primes less than 100.

D.IS There Any Formula That Generates Primes?

For centuries,mathematicians have sought a simple formula that would yield every prime number or failing this ,a formula that would produce nothing but primes.

Let us pose the problem first:”Find a function f(n) whose domain is the positive integer and whose range is some infinite subset of the set of all primes”.

It was widely believed in the middle ages that the quadratic polynomial ,due to Leonard.Euler,

$f(n)= n^2 +n+41$

assumed only prime values,but the following table evideneced that the claim is correct for n=0,1,2,3,……….,39

n	f(n)	n	f(n)	n	f(n)
0	41	14	251	28	853
1	43	15	281	29	911
2	47	16	313	30	971
3	53	17	347	31	1033
4	61	18	383	32	1097
5	71	19	421	33	1163
6	83	20	461	34	1231
7	97	21	503	35	1301
8	113	22	547	36	1373
9	131	23	593	37	1447
10	151	24	641	38	1523
11	173	25	691	39	1601
12	197	26	743		
13	223	27	797		

However this provocative conjecture is shattered in the cases for n=40 and n=41:

$f(40)=40.41+41=41^2$

f(41)=41.42+41=41.43

But again the next value f(42)=1847 turns out to be a prime again.Infact,for the first 100 integer ,Euler polynomial represents 86 primes.

We have also many formulae:

$G(n)=n^{2}+n+27941$ produces 286128 primes where $0\leq n\leq 10^{6}$

$H(n)=103n^{2}-3945n+34381$,found in 1988,produces 43 distinct primes for .

n=0,1,2,……,42

$K(n)=36n^{2}-810n+2753$ does slightly better by giving a string of 45 prime values

E.Whyshould We Run With These Polynomial?

It is astonishing to observe that the failure of the above polynomials to be prime producing is no accident….as we can easily show that "$\exists$ **No Non-Constant Polynomial F(N) With Integral Co-Efficients Which Assumes Only Primes For Integral Values of N**".

The proof is so easy that anyone may handle it on his own.So we left it as an exercise.

In recent times a measure of success has been cited in the search of prime-producing functions.W.H.Mills proved in 1947 that $\exists$ **a positive real number 'r' such that the Expression $F(N)=[R^{3^{n}}]$ Is Prime For N=1,2,3,……..**(the brackets indicates the greatest integer function).It should be noted that nothing is known about the actual value of r rather it is an existence theorem and Mill's function doesn't produce all the primes.

F.Some Remarkable Facts

Recall that in the proof of infinitudes of primes,we consider ,for each prime p,another integer $p^{\#}$ to be the product of all primes that are less than or equal to p.Then numbers of the form $p^{\#}+1$ are called the **Euclidean numbers**.If you look at them you see that the first five of them are all primes:

$2^{\#}+1=2+1$	3
$3^{\#}+1=2.3+1$	7
$5^{\#}+1=2.3.5+1$	31
$7^{\#}+1=2.3.5.7+1$	211
$11^{\#}+1=2.3.5.7.11+1$	2311

However, $13^{\#}+1=59.509$

$17^{\#}+1=19.97.277$

$19^{\#}+1=347.27953$

are not prime

Question

Can one find infinitely many primes p for which $p^{\#}+1$ is also prime?For that matter,are$\exists$infinitely many composites $p^{\#}+1$?This still an open problem in Number theory.

At present 18 primes of the above form have been searched out corresponding to p=2,3,5,7,11,31,379,1019,1021,2657,3229,4547,11549,13649,18523,23801,24049 and the largest of these a number consisting of 10387 digits which was discovered in 1995 and interestingly the integer $p^{\#}+1$ is composite for all other $p\leq 35000$.

In 1845,Joseph Bertrand conjectured that **"for all $n\geq 2$, there is at least one prime in between n and 2n",**though he was unable to establish this but verified its trueness for all $n\leq 3{,}000{,}000$.

To achieve this choosing the sequence of primes 3,5,7,13,23,43,83,163,371,631,1259,2503,4999,9973,19937,39869,79699,159389,…………,each of which is less than twice the proceeding..

Some Facts on Twin Primes

Pair of successive odd integers p and p+2 which are both primes are defined as the so-called **'Twin Prime'**.**An open problem** are there infinitely many pairs of twin primes?

So far Electronic computer have discovered 152,892 pairs of twin primes less than 30,000,000 and 20 pairs between 10^{12} and $10^{12}+10{,}000$ which hints their growing scarcity as the positive integers increase in magnitudes.The largest twin primes till date is $242206083.2^{38800}\pm 1$,each 11689 digits long,discovered in 1995.

Problem

Given any n,does$\exists$n consecutive integers all of which are composite?

After computer searches we get that following the prime 42,842,283,925,351,there is a gap of width 778 and no gap of this size exists between two smaller primes.The largest effectively calculated gap of length 864 is after the prime 6,505,941,701,960,039.

F.Goldbach's Conjecture

The most popular unsolved problem for near about 270 years is this "*GOLDBACH'S CONJECTURE*".Many mathematicians devoted their whole life for solving this problem,but each and everyone failed either to prove this or to disprove it till date.Though it is very much overwhelming that no example has yet not been found to discard this conjecture.Now what's about this conjecture?very simplest one ….In a letter to Euler in the year 1742,Christian Goldbach made a guess that "**every even integer greater than 4 can be expressed as a sum of two odd primes"….**It has been verified by computation for all even integers less than 4.10^{11} .Although this supports the feeling that Goldbach was correct in his guess but it is far from a mathematical proof.G.H.Hardy,in his address to the Mathematical Society of Copenhegen in 1921,uttered that the Goldbach's conjecture appeared "…….probably as difficult as any of the unsolved problems in Mathematics".It inspired the Hollywood industry to produce films on this conjecture and they did this and many stories been written in this context…….

2=1+1
4=2+2
6=3+3=1+5
8=3+5=1+7
10=5+5=3+7
12=5+7=1+11

14=3+11=7+7=1+13
16=3+13=5+11
18=5+13=7+11=1+17
20=3+17=7+13=1+19
22=3+19=5+17=11+11
24=5+19=7+17=11+13=1+23
26=3+23=7+19=13+13
28=5+23=11+17
30=7+23=11+19=13+17=1+29

Theorem

There is an infinite number of primes of the form 4n+3,for all natural n.

So this supplies a huge number of primes….In our next discussion we shall find a large class of primes of the form$\mathbf{2}^{n}$ **-1** which are famously known as Mersenne Primes.

G.Mersenne Primes

The numbers of the form$M_n = 2^n - 1, \forall n \geq 1,$ are called MERSENNE NUMBER due to a French monk MERIN MERSENNE(1588-1648).Nowthose MERSENNE NUMBERS which are primes are called MERSENNE PRIME.In 1644,MERSENNE erroneously stated thatM_p is prime for p=2,3,5,7,13,17,19,31,67,127,257 an composite $\forall$ primes $p < 257$.After 300year,In 1947 we came to know that M_{67} AND M_{257} are not primes but M_{61} , M_{89} ANDM_{107} entered into the list.

Mersenne stated that if n is a prime, then 2^{n}-1 is also prime but it doesn’t hold for n=11since 2^{11}-1= 2047=23$\times$89,however it can be shown that n must be prime in order for the Mersenne Number to be prime.

Theorem

If 2^{n} -1 is prime ,for some natural number n,then n itself is also a prime.

	Exponent	Expanded Version
M_1	2	$M_1=2^{2}$ -1
M_2	3	$M_2=2^{3}$-1
M_3	5	$M_3=2^{5}$-1
M_4	7	$M_4=2^{7}$ -1
M_5	13	$M_5=2^{13}$-1
M_6	17	$M_6=2^{17}$-1
M_7	19	$M_7=2^{19}$-1
M_8	31	$M_8=2^{31}$-1
M_9	61	$M_9=2^{61}$-1
M_{10}	89	$M_{10}=2^{89}$ -1
M_{11}	107	$M_{11}=2^{107}$-1
M_{12}	127	$M_{12}=2^{127}$-1

This is the list of the first twelve Mersenne primes which is whatMersenneshoud have compiled when he first presented it.

This theorem tells us that the primality of the Mersenne numbers always be checked and for this we always use the LUCAS-LEHMER testwhich is given below:

H.Lucas-Lehmer Test

The Lucas-LehmerTestis one of the most common tests to check the primality of Mersenne numbers

Lucas created this test in 1856 and it was modified later by Lehmer in 1930.

Theorem

Let p be the prime and let n = 2^{p} - 1 .Let S_1= 4 and $S_{k+1} = S_k^2 - 2$ if k ≥ 1.Then n is prime if and only if S_{p-1} is divisible by n.

$S_1 = 4$

$S_2 = 14$

$S_3 =194$

$S_4 =37,634$…..

Example:Let p=3.Then n=2^{3}-1=7 and 14$\div$7=2,thus 7 is prime.

Example:Let p=5.Then n=2^{5}-1=31 and 37,634$\div$ 31=1,214.

The examples shows that how this test works.Also note that this test only works on odd primes except one even prime 2.

I.Largest Prime Known

Due to Lucas-Lehmer test our motive is to search for the Mersenne Primes which is much easier than other.As of now we have found 44 Mersenne Primes .The largest Mersenne Prime is $M_{44}=2^{32,583,657}-1$

which consists of 9,808,358 digits and was found in 2006 by a program called the Great Internet Mersenne Prime Search(GIMPS).

J.Encryption

Primes are very much uncanny in nature which provokes us to find some good characteristic in them that gives a fruitful application towards modern civilization although they have been studied since near about 500 B.C.

Encryption is one of the ways of hiding information by turning messages into gibberish so that they can only be read by the intended recipient.When a credit card number is sent over the internet,the number is encrypted by the browser. The encryption is an algorithm based on the theory of prime numbers.In short encryption is done by multiplying two 100 digit prime numbers in order to represent the credit card number which is safe because factorizing this product could take centuries even by a high speed computer until the intended person receives the information.Encryption can be created in many different ways which is a subject todays research to make information secure and safe.

K.other Applications

There are many other applications of primes because of their unique characteristics in music ,movies and even lifecycles of insects.Prime numbers are drawn into music to create some rhythms of different tests and make the composition more attractive.

Also a less direct involvement of prime numbers is on the big screen.Manyfilms has been directed due to unusual behaviour of the primes such as The Mirror Has Two Faces and A Beautiful Mind.

L.Conclusions

We have seen a few important properties of primes that includes “Building Blocks” property ,the infinitude of primes and many other.I have discussed a little bit about the “Sieve of Erartosthenes”for searching out primes.Also I have shown a few classifications of primes amongst which Mersenne Numbers are very much prevalent because of the famous Lucas-Lehmertest.Above all the usefulness and greater interest in searching them in growing day by day due to their unique characteristics.

References

1. E. W. Weisstein. Fundamental theorem of arithmetic.MathWorld.http://mathworld.wolfram.com
2. C. Ast. Prime numbers.Mathematics and Statistics.Wichita StateUniversity.http://www.math.wichita.edu/
3. C. K. Caldwell. (2008, Feb) Why is the numbers one not prime. The Prime Pages. The University of Tennessee at Martin.http://primes.utm.edu
4. J.J. O’Connor, E. F. Robertson. (2005, Mar.) Prime numbers.TheMacTutor History of Mathemactics Archive.University of St. Andrews.http://wwwhistory. s.standrews.ac.uk/HistTopics/Prime_numbers.html
5. E. Sohn. (2008, Mar.) Prime time for cadas.Science News for Kids. http://www.sciencenewsforkids.org
6. EFF cooperative computing awards. Electtronic Frontier Foundation.http://www.eff.org/awards/coop
7. Euclid’s elements book IX, Clark University. http://babbage.clarku.edu
8. J. Fraser. (2007) Prime time. Virtual Science Fair.http://www.virtualsciencefair.org
9. C. K. Caldwell. (2008, Feb) Mersenne primes: History,theorems andlists. The Prime Pages. The University of Tennessee at Martin.http://primes.utm.edu
10. C. K. Caldwell. (2008) Euclid’s proof of the infinitude of primes.ThePrime Pages. The University of Tennessee at Martin.http://primes.utm.edu
11. D. M. Burton. Elementary Number Theory.Boston, MA, 1980, pp. 46-57.
12. D. M. Burton. The History of Mathematics.Boston, MA, 1999, pp. 465-466.
13. GIMPS home page. (2006, September 11). The Great Internet Mersenne prime search http://www.mersenne.org.