Available online at www.elixirpublishers.com (Elixir International Journal)

Applied Mathematics

Elixir Appl. Math. 88 (2015) 36296-36301

ISSN: 2229-712X

Survey on Prime Numbers

A.R.C.De Vas Gunasekara*, A.A.C.A.Jayathilake and A.A.I.Perera

Department of Mathematics, Faculty of Science, University of Peradeniya, Sri Lanka.

ARTICLE INFO

Article history:

Received: 21 September 2015;

Received in revised form:

30 October 2015;

Accepted: 06 November 2015;

Keywords

Mersenne primes,
Fermat primes,
Twin primes,
Pseudoprime,
Prime Ideals,
Sylow p – Subgroups,
Primality testing.

ABSTRACT

Primes are the building blocks of integer universe. Prime numbers plays a major role in number theory. This paper is a detailed survey on prime numbers.This describes different types of primes and some testing methods. In addition to that, we have constructed MATLAB programs using popular primality tests to determine a given positive integer is prime or not. Further, this concises the definitions regarding prime numbers, history of prime numbers, distribution of prime numbers, some mathematical occurrences and open questions concerning prime numbers. Moreover, the usage of primes in nature and in the real life has been considered.

Introduction

A prime number or simply a prime is a natural number greater than 1 that has no positive divisors other than 1 and itself.symbolically, a number p is said to be prime if

(i) p > 1

(ii) p has no positive divisors except 1 and p.

A prime number is an integer greater than 1, only having two factors, 1 and itself. [1]

Another definition for prime numbers has been given by Borevich and Shafarevich as an element p of the ring **D**, nonzero and not a unit, cannot be decomposed into factors p=ab neither of which is a unit in **D**, in their classic text "Number Theory" . It is well known that $2, 3, 5, 7, 11, 13, \ldots$are the first few primes. A natural number greater than **1** that is not a prime is called as a composite number. The property of being a prime is known as *primality*. And two numbers **a** and **b** are said to be *relatively prime* if they have no prime factors in common.

History and revolution of Prime numbers

There are some hints that ancient Egyptians had an idea of prime numbers. But they had different definitions for primes and composites than what we talk today. However, it is a known fact that the ancient Greek mathematicians were the first to study prime numbers and their properties during 300 B.C.

Then the Great Greek mathematician Euclid came up with that there are infinitely many prime numbers. This achievement can be taken as the beginning of the abstract theory of prime numbers. Euclid has used a method of contradiction to prove that there are infinitely many prime numbers.

Assume that the primes are finite in number, and denote by p the largest. Consider one more than the product of all primes, namely, n=(2,3,5,….p)+1. [1] Now, **n** cannot be divisible by any of the primes **2** through p, because any such division leaves remainder **1**. But we have assumed that the primes up through p comprise all of the primes. Therefore, n cannot be divisible by any prime. So the assumption of primes are finite in number is contradicted. That is, numbers of primes are infinite.

Another valuable fact which has been proposed by Euclid is the Fundamental Theorem of Arithmetic (FTA), also known as unique factorization. This says that every positive integer greater than 1 is either a prime or a product of primes in a unique way. So there is no doubt that the primes are the building blocks of positive integers.

Sometimes later in 200 B.C, a Greek mathematician Eratosthenes created an algorithm, known as the Sieve's method for calculating primes up to a specified integer. Further, Gauss, Fermat and Mersenne made remarkable contributions to this prime number field. H.G Hardy, an English mathematician was the latest to study on prime numbers.

Hence, there are several classes of prime number such as,

Mersenne primes: Primes of the form of 2^p-1 where p is also a prime,

Fermat primes: Primes of the form of $2^{2^n}+1$ where n is a positive integer,

Twin primes

Appear in two sides of an even number p and p+2, ex: - 3&5,5&7……

Tele: +94717493055
E-mail addresses: ajani.gunasekara@gmail.com

Sexy primes

Difference is 6, i.e. p and p+6, ex: - 11&17,17&23….[1]

With the development of network security and public key cryptography, interest of findin g the large prime numbers and studying the properties of primes rapidly increased. Some companies and organizations are offering cash prizes for large prime numbers .

As of December 2014, the largest known prime number is $2^{57,885,161} - 1$, which is a Mersenne prime.

Since 1951, all the largest known primes have been found by computers. The search for ever larger primes has generated interes st outside Mathematical circles. The *Great Internet Mersenne Prime Search* (GIMPS) and other distributed computing projects to find large primes have become popular in the last ten to fifteen years, while several mathematicians continue to struggle with the theory of primes.

Distribution of prime numbers

We know that there are infinitely many primes, but can we propose an equation to find the n^{th} prime. Still it is a problem to be solved. There is no exact pattern of primes among composites, hence, they are random. However, in 1792, Gauss approximated a pattern which is the path to prime number theorem.

In number theory, the *Prime Number Theorem* (PNT) describes the asymptotic distribution of the prime numbers. The PNT gives a general description of how the primes are distributed among the positive integers. It formalizes the intuitive idea that primes become less common as they become larger.

In PNT, it states that, $\pi(x)$ as the prime-counting function that gives the number of primes less than or equal to *x*, for any real number *x*, where $\pi(x) \sim \frac{x}{\ln x}$

Moreover, it states that if a random integer is selected in the range of zero to some large integer N, the probability that the selected integer is prime is about $1 / ln(N)$, where $ln(N)$ is the natural logarithm of N. Consequently, a random integer with at most 2^n digits (for large enough n) is about half as likely to be a prime as a random integer with at most *n* digits.

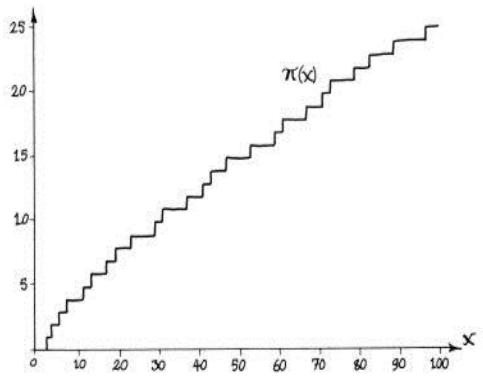


Figure 1. The diagram that illustrates the distribution of primes

Some mathematical occurrences of primes

Prime Ideals

An Ideal I of ring R is a subring satisfying the condition, ra ∈ I and ar ∈ I ∀ r ∈ R and a ∈ I [15]

Let P be an Ideal in ring R , P is called as a *Prime Ideal* if ab ∈P ⇒either a∈P or b∈P. If p is a prime number, then pZ = {pn| n ∈Z} is a Prime Ideal.

Sylow p-Subgroups

Let p is a prime number, then, a subgroup H of a group G is called a *p - subgroup* of G , if the order of each element of H is a power of p .[15]

For a given prime p and a given finite group G a Sylow p-subgroup of G is a maximal p-subgroup of .[15]

If G is a non-trivial group, a proper subgroup M of G is said to be a "*maximal subgroup*" of G, if there is no subgroup L of G s.t. $M < L < G$.

Primes in nature

Cicada's life circle has a connection between prime numbers. Cicada, a certain type of insect lives underground and reappearing after 7, 13 or 17 years, at which point they fly about, breed, and then die after a few weeks at most. Note that, 7,13,17 are prime numbers. The reason behind this $_{7,13,17}$ year period is that to avoid predators. Assume that a cicada' appeared at non-prime number intervals, say every 10 years, then predators appearing every 2, 5, or 10 years would be sure to meet them.

In 20^{th} century, a great mathematician *Stanislaw Ulam* discovered amazing design considering density of prime numbers which is known as *Ulam's rose* or *prime number spiral*. It is similar to some pattern that can be seen in nature, simply a rose. [9]

Primes are the building blocks of all the numbers. If primes are atoms, then other numbers are like molecules. There is Chemistry in prime numbers. Since primes are like atoms we can write chemical formula for composite numbers. For an example, chemical formula for water is H_2O, like that chemical formula for 12 can be written as $2^2 \times 3$ where 2 and 3 are primes. [5] [7]

Prime Conjectures

There are number of open questions and conjectures on prime numbers. Here are some of them; [6]

(i) *Goldbach's Conjecture*: Every even $n > 2$ is the sum of two primes.

(ii) *The Odd Goldbach Problem*: Every odd $n > 5$ is the sum of three primes.

(iii) Every even number is the difference of two primes.

(iv) *Twin Prime Conjecture*: There are infinitely many twin primes.

(v) Are there infinitely many primes of the form n^2+1?

(vi) The number of *Fermat primes* is finite.
(vii) Is there always a prime between n^2 and $(n+1)^2$?

Primality testing methods [13] [14] [9]

Primality test is a test or an algorithm to check a given positive integer is prime or composite.

Two categories can be found in primality testing, such as *deterministic* and *probabilistic*. Deterministic tests are designed to determine a positive integer is prime or not with certainty while probabilistic tests consist of sequence of tests.

The *Sieve's method* and *Wilson's theorem* are [1] [5] examples for deterministic primality tests. They provide a reliable answer whether a number is prime or not while test based on Fermat's little theorem. Chinese primality test are examples for probabilistic primality tests.

Probabilistic tests do not give the certainty that a number satisfying its conditions is a prime. If a composite number satisfies the conditions of a certain probabilistic test then it is known as a "*pseudoprime*".

There are many types of pseudoprimes. Such as *Fermat pseudoprimes* or *base-a pseudoprime* which consist of composite numbers that satisfy Fermat's little theorem. Further, *Lucas pseudoprimes* contains composite numbers which satisfy Lucas test and *base-2 pseudoprim* has composite numbers that satisfy Chinese Primality test.

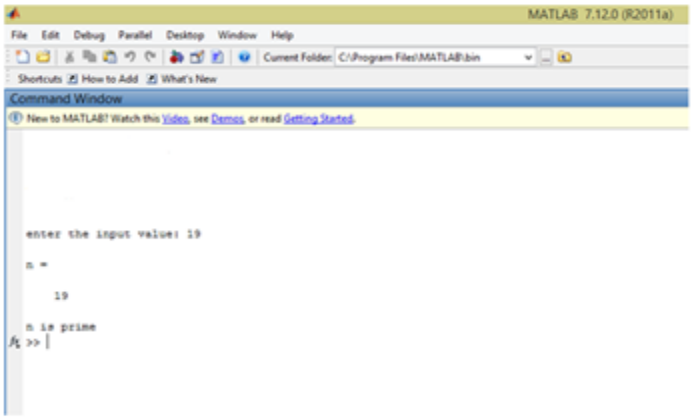
In this both type of tests, what we have to do is:
(i) Pick a random positive integer greater than 1 or take a desired number.
(ii) Choose a primality test/algorithm (Deterministic or probabilistic) according to available resources.
(iii) Perform calculations or check conditions (manually or using computers).
(iv) Get the result. (whether the input is prime or not)

Wilson's Theorem

This theorem indicates that the necessary and sufficient condition for an integer n to be a prime is,
$(n-1)! \equiv -1 \pmod{n}$. [3]

Wilson's theorem is a deterministic primality test as mentioned above. But this test is not practical when n is large, because it is difficult to calculate (n-1)! manually.

The idea of this test can be implemented using MATLAB.



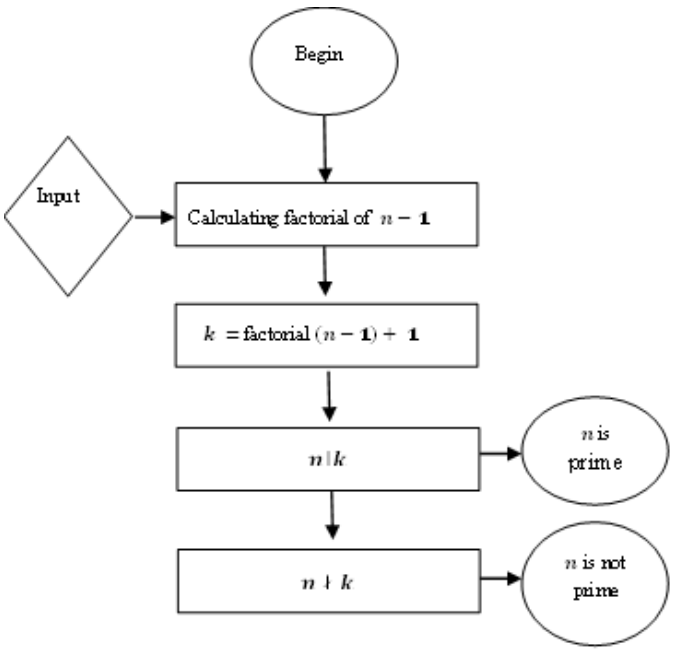


Figure 2. Diagram of the MATLAB program for Wilson's Test

Sieve of Eratosthenes (Sieve's Method)

This algorithm is based on a simple observation that, if n is composite, then n has a prime factor less than or equal to $\sqrt{n}$. [1]

Using this method we can get a prime number list up to some positive integer. Let n be a positive integer greater than 1 and suppose that you want to get a prime number list from 2 to n. Then circle all the prime numbers less than or equal to $\sqrt{n}$ and cross off all the multiples of them. Then the remaining are the primes up to n.

But this method is not that efficient as when n is a large numbers, it is difficult to implement. Sieve's method is a deterministic method for which does not involve probability and the answer can be accepted directly.

Chinese primality test

Ancient Chinese mathematicians discovered that if p is prime, then 2^p-2 is divisible by p. This means ,

$2^p \equiv 2 \ (mod\ p)$ [1] [5]

Every prime number is in this form, but positive integer satisfying this condition can or cannot be a prime. There is a possibility that positive integer satisfying this condition can be a composite. A composite number k satisfying $2^k \equiv 2 \ (mod\ k)$ is known as a *base-2 pseudoprime*. This method is a probabilistic method.

Chinese primality theorem: Let n be an integer, n>1

If $2^n \equiv 2 \pmod n$, then n is either a prime or a base-2 pseudoprime.

We can use this as a probabilistic primality test. That is if p is a prime then it should satisfy $2^n \equiv 2 \pmod n$.

Fermat's primality test

This method is a modified version of Chinese primalty test, which is also a probabilistic test. In Chinese primlity test, 2 was taken as the base and in this method, no restrictions are for the base and hence, any positive integer can be used as as the base element.

Fermat's little theorem says that if p is a prime, and **a** be any positive integer and if (p ,a) = 1 then $a^{(p-1)} \equiv 1 \pmod p$.

(i.e. $a^p \equiv a \pmod p$ Since (p ,a) = 1 [3]

Now, Fermat's little theorem can be modified to a primality test asan odd positive integer **n** is composite if there exists a positive integer **a** such that (a,n) = 1 and $a^{(n-1)} \not\equiv 1 \pmod n$.

Also, the contrapositive way of Fermat's primality test can be used. If any composite number satisfies the condition of Fermat's little theorem, it is known as a base _ a pseudoprime. This test is also can be implemented in MATLAB.

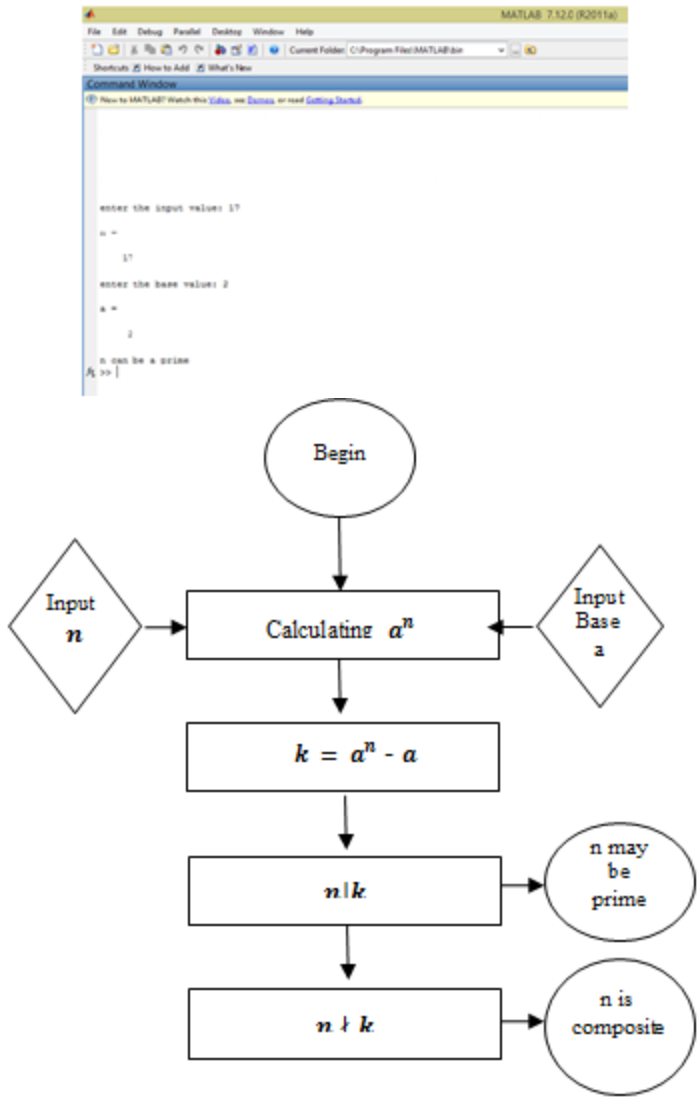


Figure 3. Diagram of the MATLAB program for Fermat's Test

Lucas test

This test involves a certain type of numbers known as *Lucas Numbers.*

Lucas numberis asequence of integers L_n defined by the linear recurrence relation

$$L_n = L_{n-1} + L_{n-2}$$

with $L_1 = 1$ and $L_2 = 3$

Solving the above recurrence relation gives L_n in terms of n as follows: Let $L_n = a^n$ then we have

$$a^n = a^{n-1} + a^{n-2}$$
$$\Rightarrow a^n - a^{n-1} - a^{n-2} = 0$$
$$\Rightarrow a^{n-2}(a^2 - a - 1) = 0$$
$$\Rightarrow a^2 - a - 1 = 0 \Rightarrow a = \frac{(1 \pm \sqrt{5})}{2}$$

Then, $L_n = A((1+\sqrt{5})/2)^n + B((1-\sqrt{5})/2)^n$ where *A* , *B* are arbitrary constants.

Finding *A* and *B*,

$L_1 = 1 = A((1+\sqrt{5})/2)^1 + B((1-\sqrt{5})/2)^1$ → (1)

$L_2 = 3 = A((1+\sqrt{5})/2)^2 + B((1-\sqrt{5})/2)^2$ → (2)

By Solving (1) and (2), we get *A* = 1 and *B* = 1

So $L_n = ((1+\sqrt{5})/2)^n + ((1-\sqrt{5})/2)^n$ is the n[th] Lucas number.

Lucas test states that if n is prime then $L_n \equiv 1 \ (mod\ n)$,

where $L_n = ((1+\sqrt{5})/2)^n + ((1-\sqrt{5})/2)^n$.

This method is also a probabilistic method. A composite number which satisfies Lucas test is known as *Lucas pseudoprime*.

Real Life Applications of Prime numbers

There are several direct applications of prime numbers, but most can be found in the field of *Information Technology*. Among them, creation of public key cryptography algorithms, in hash tables, in pseudorandom number generators and for rotor machines are some applications of prime numbers. [12] [5]

Previous work regarding primes

Jovan Jovenčević in his research paper named as "*Finding prime numbers*" has made an overview of the primality testing algorithms. Complexity, time performance, and the accuracy of each of the algorithms were analyzed. For that purpose, extensive experiments were performed. Algorithms were implemented in the programming language Java. [21]

Zachary S. McGregor-Dorsey has discussed the most popular methods of primality testing, along with some intermediate steps of their formulation. Also, he has analyzed the importance of primality testing, the history of prime numbers, and the difficulties of implementing these tests. Especially he has concentrated on Lucas sequences and the Lucas test in his research paper – "*Methods of Primality Testing*". [13]

Carl Pomerence in his research paper called "*Primality Testing: Variations On A Theme Of Lucas*" indicated an idea of Edouard Lucas that is a common element in various primality tests. These tests include several facts based on Fermat's little theorem, elliptic curves, Lucas sequences, and polynomials over finite fields, including the recent test of Agrawal, Kayal, and Saxena. [10]

Moreover, Dianne M. Lee has given a short introduction to primes, Sieve's method, twin primes and the history of prime numbers while he has concentrated more on current interest for primes with the development in public key encryption. Furthermore he has stated that there is money in primes in his research paper – "*What's so amazing about Primes?*" [20]

In Jerry Crow's "*Prime Numbers in Public Key Cryptography - An Introduction*", he has stated the use of public-key cryptography in the information protection and privacy arenas. Further, he says that Public key cryptography algorithms utilize prime numbers extensively.

This paper provides an introduction to prime numbers and how they are chosen, identified and used in public key systems. The content of this paper is specifically targeted at an audience that has only basic mathematical knowledge. The objective of this paper is to inform the mainstream information security professional – who does not necessarily possess an extensive knowledge of mathematics – about the nature of prime numbers and how they are used in contemporary public key systems, thereby increasing their overall understanding of contemporary asymmetric encryption algorithms. As a part of his investigation, the basic elements of Diffie - Hellman exchange and the RSA algorithm are explored. [24]

David J. Wirian has proposed a method to find a large prime number using some prime sieve techniques using parallel computation. Also, he has compared the techniques by finding the results and the implications in his research paper called "*Parallel Prime Sieve: Finding Prime Numbers*".[16]

Chris K. Caldwell and Yeng Xiong have answered the question "*What is the first prime*"? It seems that the number two should be the obvious answer, and today it is, but it was not always so. There were times when and mathematicians for whom the numbers one and three were acceptable answers. To find the first prime, we must also know what the first positive integer is. Surprisingly, with the definitions used at various times throughout history, one was often not the first positive integer (Some started with two and a few with three). Moreover they have surveyed the history of primality of one, from the ancient Greeks to modern times. Further, they have discussed some reasons of changes in definitions, and provided several examples. Also, provided some information on the last significant mathematicians, to list the number one as prime. [17]

The Elementary Proof Of The Prime Number Theorem: An Historical Perspective by D. Goldfeld is an abstract research paper regarding prime number theorem and prime distribution. [18]

Efficient generation of Prime Numbers by Marc Joye, Pascal Paillier and Serge Vaudenay discuss that the generation of prime numbers underlies the use of most public-key schemes, essentially as a major primitive needed for the creation of key pairs or as a computation stage appearing during various cryptographic setups. Surprisingly, despite decades of intense mathematical studies on

primality testing and an observed progressive intensification of cryptographic usages, prime number generation algorithms remain scarcely investigated and most real-life implementations are of rather poor performance.

Also they have showed that the common generators typically output a n-bit prime in heuristic average complexity $O(n^4)$ or $O(n^4/\log n)$ and these figures, according to experience, seem impossible to improve significantly: this paper rather shows a simple way to substantially reduce the value of hidden constants to provide much more efficient prime generation algorithms.

Another part of this work is that they have applied their techniques to various contexts (DSA primes, safe primes, ANSI X9.31-compliant primes, strong primes, etc.) and showed how to build fast implementations on appropriately equipped smart-cards, thus allowing on-board key generation. [19]

Jeff Young's "*Large Primes And Fermat Factors*" is a research paper proposing a systematic search for large primes has yielded the largest Fermat factors known. [22]

Finally, Manindra Agrawal, Neeraj Kayal and Nitin Saxena have presented an unconditional deterministic polynomial-time algorithm that determines whether an input number is prime or composite, in their research paper called "*Primes is in P*" [23]

Conclusion

This is a deep study on prime numbers. In this article, properties of prime numbers, different types of prime numbers and their real life applications as well as the applications in nature have been analyzed. Furthermore, different types of primality tests have been studied and also MATLAB programs for each of those tests have been constructed. Moreover, a summary of previous work regarding primes have been included.

References

[1] G.H. Hardy and E.M Wright, An Introduction to the Theory of numbers, Oxford press.
[2] Andrew S. Tanenbaum, Computer Networks .
[3] MATLAB overview & MATLAB Documentation at Math Works website.
[4] Richard Crandall and Carl Pomerance , Prime Numbers, A computational perspective, 2nd edition .
[5] Dr. Chris K. Caldwell, University of Tennessee , USA, Prime pages .
[6] Ajay Chaudhuri, Introduction to Number Theory.
[7] W. Eric Weisstein, "Lucas Number." From *Math World*--A Wolfram Web.
Resource. *http://mathworld.wolfram.com/LucasNumber.html* .
[8] Harvey Dubner and Wilfrid Keller, Factors of Generalized Fermat Numbers.
[9] Mathematics of Computation, Vol. 64, No. 209 (Jan., 1995), pp. 397-405, Published by: American Mathematical Society, Article Stable URL: *http://www.jstor.org/stable/2153343*.
[10] Carl Pomerance, Primality Testing: Variations on a theme of Lucas.
[11] *www.mersenne.org*
[12] Jerry Crow, SANS Institute, Reading room, Prime Numbers in Public Key Cryptography, An Introduction.
[13] Zachary S. McGregor-Dorsey, Methods of Primality Testing.
[14] Manindra Agrawal, Is n a Prime Number? , IIT Kanpur, March 27, 2006, Delft.
[15] M.R Adhikari, Text Book of Linear Algebra: An Introduction to Modern Algebra, 2004 Allied publishers Pvt Ltd.
[16] David J. Wirian, Institute of Information & Mathematical Sciences, Massey University at Albany, Auckland, New Zealand, Research paper on Parallel Prime Sieve: Finding Prime Numbers.
[17] Chris K. Caldwell, Yeng Xiong – "What is the smallest prime?" , Journal of Integer Sequences, Vol. 15 (2012), Article 12.9.7 .
[18] D. Goldfeld, The Elementary Proof Of The Prime Number Theorem: An Historical Perspective.
[19] Marc Joye, Pascal Paillier, Serge Vaudenay, Efficient Generation of Prime Numbers, CHES 2000, vol. 1965 of Lecture Notes in Computer Science, pp. 340{354, Springer-Verlag, 2000}.
[20] Dianne M. Lee, What's So Amazing About Primes? ,
Department of Mathematics, University of Nebraska-Lincoln, July 2011.
[21] Jovan Jovenčević, Finding Prime Numbers – Internal Assessment in Mathematics, June 10,2013.
[22] Jeff Young, Large Primes and Fermat Factors, American Mathematical Society, Mathematics of Computation, Vol. 67, No. 224 (Oct., 1998), pp. 1735-1738.
[23] Manindra Agrawal, Neeraj Kayal, Nitin Saxena, PRIMES is in P, IIT Kanpur.
[24] Jerry Crow, Prime Numbers in Public Key Cryptography; An Introduction, SANS Institute 2003.