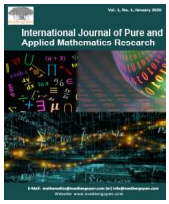
https://doi.org/10.51483/IJPAMR.2.1.2022.65-73 ISSN: 2789-9160

SvedbergOpen
DISSEMINATION OF KNOWLEDGE

International Journal of Pure and Applied Mathematics Research

Publisher's Home Page: https://www.svedbergopen.com/



Research Paper Open Access

A Theoretical Approach on Deterministic and Probabilistic Prime Numbers

Sumit Tiwari[1*] and Atin Kushwaha[2]

[1]Department of Computer Science and Engineering, Rajkiya Engineering College, Kannauj, Uttar Pradesh, India. E-mail: tsumit1199@gmail.com

[2]Department of Computer Science and Engineering, Rajkiya Engineering College, Kannauj, Uttar Pradesh, India. E-mail: atinkushwaha2000@gmail.com

Article Info

Volume 2, Issue 1, April 2022
Received : 18 June 2021
Accepted : 22 February 2022
Published : 05 April 2022
doi: 10.51483/IJPAMR.2.1.2022.65-73

Abstract

This survey paper is based on prime numbers and primality test. Prime numbers are building block of number theory. Prime numbers play a vital role in number theory, there applications are mostly found in cryptography. It is very difficult to find whether a number is prime or not whenever the number is too big. To overcome this problem there are various algorithms. This paper is written in context of prime numbers that explains about prime and some of their testing methods like Fermat's primality test, AKS Algorithm, Chinese primality test and also the Lucas test.

Keywords: *Prime numbers, Number theory, Cryptography, Algorithms*

1. Introduction

The topic prime number is of great importance in mathematics and saying particularly in the number theory, so there is a need of learning about the primes. Can you guess the largest prime number? What about 9633333333333331? The property of being a prime number for a number is known as primality (Williams, 1982 and 1984).

In this nature, numbers exist in only two types either prime or composite (except 1). The natural numbers which are greater than 1 but have factors more than 2 are known as composite numbers (Gunasekara *et al.*, 2015; Lenstra, 1981; and Bernstein., 2004). Examples are 6, 8, 9, 12… etc.

Now talking about the prime, those numbers which have only two factors, first is itself and the other is 1, are said to be prime numbers. Examples are 3, 5, 7, 11, 13… etc. Or one can also say that Prime numbers are those natural numbers (>1) which are divisible by 1 and itself. 2, 3, 5, 7, 11, 13, 17 are few prime numbers (Lenstra, 1990).

Primes can also be described as if the number *m*, is divided by every number $2 \leq \sqrt{m}$ if it divides then it is a composite number otherwise it is a prime number. The idea about prime numbers started many centuries ago by Euclid. He stated that prime numbers are infinite in number. There is no formula described by which one can relate the prime and composite numbers, since number of digits in prime is inversely proportional to the probability of that number to be a prime.

* *Corresponding author: Sumit Tiwar, Department of Computer Science and Engineering, Rajkiya Engineering College, Kannauj, Uttar Pradesh, India. E-mail: tsumit1199@gmail.com*

The interesting fact about number "2" is that it is the only even prime and also considered as the first in the list. There is one slow method by which we can check primality of a number *n,* known as trial version. In this method, we test whether number *n* is multiple of any positive integers between 2 to $\sqrt{n}$. Some questions about prime numbers have still no answers (Akgul *et al.*, 2006).

It include Goldbach Conjecture, all even integers which are greater than 2 can be written as addition of two primes (Hua, 2009), other is Twin Prime Conjecture, it states that there are infinitely many pair number of primes having one even number between them. When we write a number as a product of prime it is called prime factorization of the number.

For example:

$n = 323$

$323 = 17 * 19$

The term in the product are known as prime factors (Dixon, 1984).

Twin Prime: When the difference between two prime is less than or equal to 2. Example: (41, 43), (3, 5), (5, 7) etc. (Heath-Brown, 1982).

Cousin Prime: When the difference between two prime is 4. Example: (3, 7), (7, 11) etc.

Balanced Prime: Prime numbers which is in between two prime means the difference between them is constant. Example: (53) as difference between 47 and 53 is equal to difference between 53 and 59 etc. (Bombieri and Harold, 1966).

Palindromic Prime: If the prime number is found to be a palindrome. Example: 101,131,151 etc.

Reversible Prime: Primes which are reversed in order to get a prime. Example: 13, 31, 17, 71 etc.

Pythagorean Primes: Primes which are sum of square of two numbers. Example: 5 as 2^2 plus 1^2 etc.

Permutable Primes: Primes in which if the numbers are permutated then it is still a prime. Example: 113, 131, 97 and 79 etc.

Fermat Prime: It is also a prime number. A Fermat number F_ρ is of the form 2^m+1, where m is the p^{th} power of 2 (that is, m=2^p, where p is integer).

Mersenne Primes: Primes which can be written in the form of 2^n–1, for n is prime. Example: 2, 3, 5, 7, 13, 17 etc. (Crandall and Carl , 2006).

Sexy Prime: When the difference is 6 between two primes. Example: 11&17, 17&23 etc.

2. Literature Survey

There are two approaches, namely, 'deterministic' and 'probabilistic'. In which the deterministic means to determine whether the number is prime or not with certainty. In probabilistic approach, the outcome of the experiment is uncertain.

2.1. Trial Division

First we consider a number n, then check whether any number m from 2 to $\sqrt{n}$ divides (remainder = 0). If n is divisible by any m then n is a composite number otherwise it is prime. For example consider N = 100,

$m = 2, 3, 4, 5, 6, 7, 8, 9, 10$

N%2 = 0 so 100 is not a prime number, it is a composite number.

2.2. Wilson's Theorem

It is a deterministic primality test, which states that if a number is prime then it must follow:

$(n-1)! \equiv -1 \ mod \ n$

2.2.1. Algorithm: Wilson's Theorem

Step 1: Input the number.

Step 2: Calculate its factorial of $n-1$.

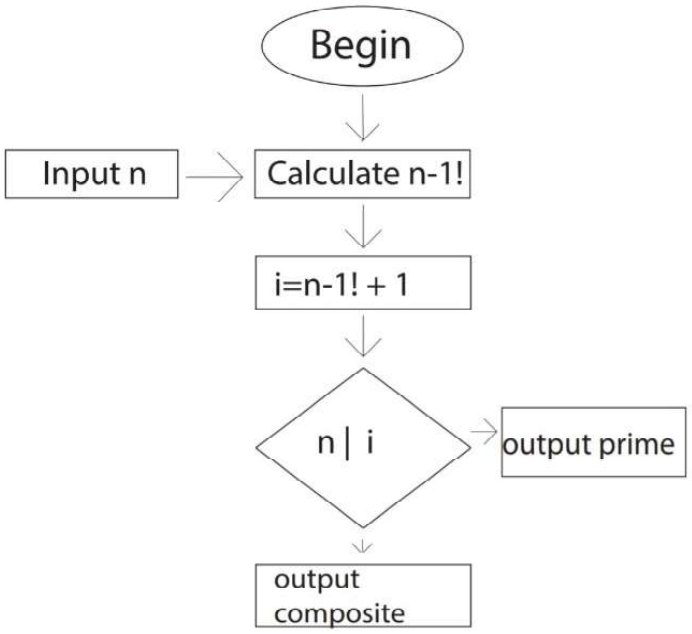


Figure 1: Wilson's Test

Step 3: Add one store it (say l).

Step 4: If *n* is divided by l then it is not prime else print prime.

2.3. Seive Method

It is also a deterministic primality test, according to this we should create a list up to the number and then marking the numbers which are divisible by some other numbers (except 1 and itself).

2.3.1. Algorithm: Seive Method

Step 1: Create a list of numbers from 2 to *n*.

Step 2: From number 2 start marking the number which are divisible.

Step 3: Increase the number by 1, repeat step 2.

Step 4: Some numbers are not marked these are primes up to *n*.

2.4. Chinese Primality Test

It is a probabilistic primality test, which states that a number (K) being prime then 2^K is divisible by K or we can write it mathematically as: $2^K \equiv 2 \; mod \; K$.

It is not very successful because some composite numbers also pass this test. Example: 341, 561, 645, 1105, 1729, and 1905 (under 2000).

2.5. Miller Rabin Primality Test

Is *n* prime?

$n - 1 = m * a \wedge k$

If $k = 1$ than number is composite

$t = a \wedge m \; (mod \; n)$

For ($p = 1$ to $k - 1$)

{

$t = t \wedge 2 \; (mod \; n)$

If ($t = +1$)

Return composite

If ($t = -1$)

Return prime

}

Example: $n = 27, a = 2$

$n - 1 = m * a \wedge k$

$27 - 1 = m * a \wedge k$

$26 = m * a \wedge k$

$13 * 2 \wedge 1 = m * a \wedge k$

$m = 13, k = 1$ since $k = 1$ number is composite

Example: $n = 61, a = 2$

$n - 1 = m * a \wedge k$

$61 - 1 = m * a \wedge k$

$60 = m * a \wedge k$

$15 * 2 \wedge 2 = m * a \wedge k$

$m = 15, k = 2$

$t = a \wedge m \ (mod\ n)$

$t = 2 \wedge 15 \ (mod\ 61)$

$t = 11$

$t = t \wedge 2 \ (mod\ n)$

$t = 11 \wedge 2 \ (mod\ 61)$

$t = 60$

Since t is not equal to $10\ r - 1$

We have to find $t - n$, $60 - 61 = -1$

Number is prime

2.6. Algorithm: Miller Rabin Test

Step 1: Miller Rabin (n, s)

Step 2: For $j = 1$ to s

a = random $(1, n - 1)$

Step 3: If witness (a, n)

Return composite

else Return prime

Witness (a, n)

Step 1: Let t and u be such that $t > = 1$, u is odd, $n - 1 = 2 \wedge t * u$

Step 2: $x_o = modular - exponentiation\ (a, u, n)$

Step 3: For $I = 1$ to t

$x_e = x^p - 12 * mod\ n$

Step 4: If $xi == 1$ and $xi - 1! = 1$ and $xi - 1! = n - 1$

Return true

Step 5: If $xi! = 1$

Return true

Return false

2.7. Fermat Primality Test

It is also a probabilistic primality test, it is nothing but a generalized form of Chinese Primality test (Brent, 1990). The only difference is that 2 was used in the Chinese primality test but here in Fermat's we will use a general base so mathematically it is: $A \wedge K \equiv A \ mod \ K$, where A is any positive number and K is prime.

Is p prime?

$a^p - a \leftarrow$ if p is prime then this number is multiple of p

$\{1 <= a < p\}$

Example $p = 5$

$1^5 - 1 = 0$

$2^5 - 2 = 30$

$3^5 - 3 = 240$

$4^5 - 4 = 1020$

Since every number is multiple of p, the number p is said prime.

2.8. Algorithm: Fermat Primality Test

Step 1: Start algorithm

Step 2: Read variable p, a

Step 3: Repeat $\{1 <= a < p\}$

{

$a^p - a$

}

Step 4: If every value $a^p - a$ is multiple of p, print p is prime

Else print number is not prime

Step 5: Stop algorithm

2.9. Lucas Test

It is also probabilistic method which states that if K is a prime number then, $L_K \equiv 1 \ mod \ K$: where $L_K = (((1 + \sqrt{5})/2) \wedge K + ((1 - \sqrt{5})/2) \wedge K)$, the numbers which pass this test may or may not be prime, known a pseudo-prime (Pomerance, 2010; Morain, 1993; and Wells, 2005).

2.10. AKS Algorithm

Agrawal *et al.* (2004) from IIT Kanpur proposed a deterministic method to say about a number to be prime or not without any condition (Agrawal *et al.*, 2004), according to them if all the coefficient of $(x - 1)^p$ $(x^p - 1)$ is a multiple of p then p a prime number (Šleževiciene *et al.*, 2004; Gordon, 1998). This algorithm is the first algorithm which deterministically refer a number to be prime or composite within polynomial time. The authors of AKS algorithm has won Gödel prize and Fulkerson prize in 2006 for their excellent work.

Is p prime?

$(x - 1)^p - (x^p - 1)$

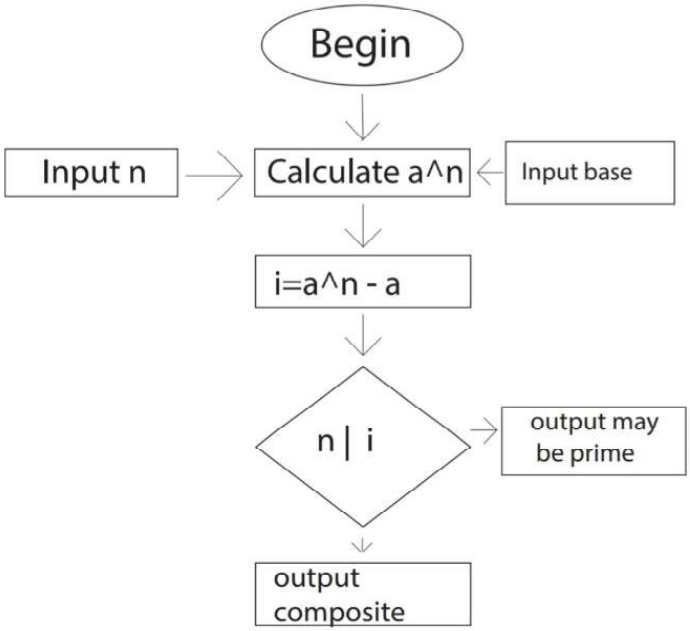


Figure 2: Fermat's Test

If all coefficient of equation is multiple of p, then p is prime

Example: $p = 3$

$(x-1)^3 - (x^3 - 1)$

$= (x-1)(x - 2x + 1) - (x^3 - 1)$

$= x^3 - 3x^2 + 3x - 1 - (x^3 - 1)$

$= -3x^2 + 3x$

Since all coefficient of equation is multiple of p, so number is prime.

2.11. Algorithm: AKS Method

Step 1: Start algorithm

Step 2: Read p which has to be checked

Step 3: $(x-1)\,\hat{}\,p - (x\,\hat{}\,p - 1)$

Step 4: If (equation is multiple of p)

Print number is prime

Else

Number is not prime

Step 5: Stop algorithm.

Real Life Application: Since prime numbers having very unique feature we can use them in public key cryptography (Kandola, 2013; Couveignes *et al.*, 2012; Hussein *et al.*, 2016), in generating pseudo-primes and also in different types of machine (Ingham and Albert, 1990; Bernstein, Daniel J., 2004). The best example of prime numbers can be seen in our mother nature, the life cycle of cicadas (a type of insect). Cicadas appears during prime number intervals—7 years, 13 years and 17 years. Even the candy crush (android gaming app) is also based on certain theory and principal of prime numbers.

We use the prime number in communication and in making the files more secure. We can also make our server more secure by using encryption and decryption, as the primes are very unique in nature and not very obvious. Prime number

help in the generation of hashes which is used by some companies and security services to provide much more security to the databases created by the Indian government or the Indian security agencies.

We also use prime number in generating the random numbers and error correcting code.

3. Analysis

Here in the Figure 3 the vertical axis shows the whole numbers and the horizontal axis shows the primes, it is normally showing that there are about 200 primes in 1200 whole numbers. In the graph we plotted the prime numbers from 2 to... (200 in number), that makes the whole numbers go up to 1200. This change is very large and it also does not get any relation with the whole numbers so that we cannot predict the next prime number.

Let us break the graph in 3 segments the first one is from 1 to 100 in the y-axis here we can see that it is very dense and the probability of finding a prime number is very high that the other two segments. In the first segment we will easily find the primes.

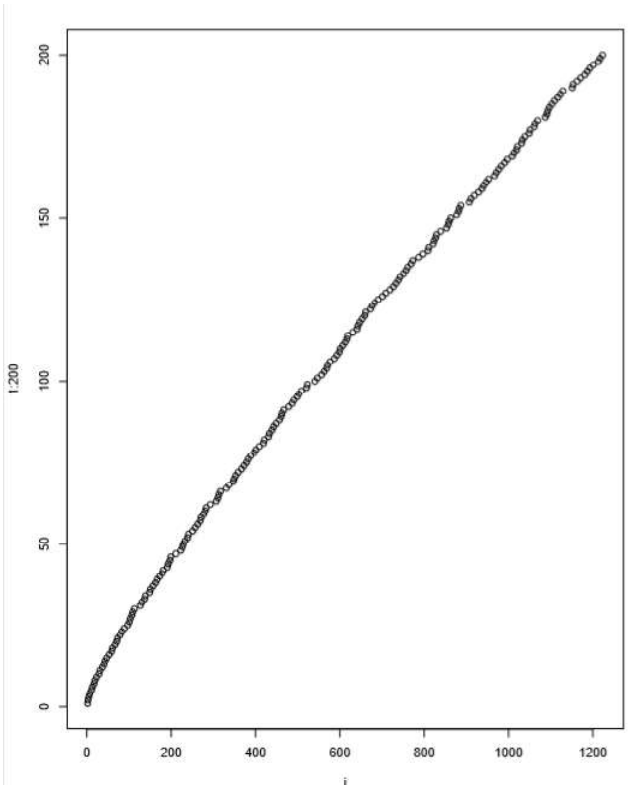


Figure 3: Distribution of Prime Over Whole Numbers

Table 1: Comparison and Analysis of Different Primality Test

Primality Test	Complexity	Probabilistic	Deterministic
Wilsons Theorem	O(n)	No	Yes
Trial Division	O(n1/2)	No	Yes
Seive Method	O(n log (log n))	No	Yes
Miller Rabin	O(log n)	Yes	No
Fermats Primality Test	O(m log n)	Yes	No
Lucas Test	$O(n^2 \log n \log (\log n))$	Yes	No
AKS Algorithm	O(log5 n)	No	Yes

N moving on to the next segment that is from 100-150 here the above graph is somewhat more discontinuous that the previous segment and with the discontinuity, it means that there is a jump in the whole number.

By the jump in the whole number it means the probability of finding a prime number is not as good as the previous one now talking about the third and last segment here we can see that the graph is more discontinuous and sudden jumps are there. In the last segment the probability of finding a prime number is quite low as compared to the last two segments. By the above observation we can say that the probability of finding a prime number is very low as we go higher in the whole number.

4. Conclusion

Prime number problems are very interesting and good for research purpose also. A lot of work have to be done in this field. The largest prime number is $2^{74,207,281}-1$ (according to GIMPS), but since infinite is there we can think there will be a prime number which will be greater than $2^{74,207,281}-1$.

Prime number have a very vast and interesting topic that's why it is also good for research works. There are many things yet to be discovered in this field. Talking about this, it is a deep study on prime, their types and different types of primality test present out there, and also the real-life application of primes are discussed. Truly saying the algorithm which takes less time or the algorithm which have less complexity is more preferable in our case that comes to be the AKS algorithm, as it is the latest of them all and is also the less complex and easy to understand and calculate.

References

Agrawal, Manindra., Neeraj Kayal, and Nitin Saxena. (2004). PRIMES is in P. *Annals of mathematics*, 160(2), 781-793.

Akgul, Bilge, E.S. *et al.* (2006). Probabilistic CMOS Technology: A Survey and Future Directions. *Very Large Scale Integration*, IFIP International Conference on. IEEE.

Bernstein, Daniel, J. (2004). Distinguishing Pime Numbers From Composite Numbers: The State of the Art in 2004. URL: http://cr. yp. to/papers. html# prime2004, 23.

Bombieri, E. and Harold, Davenport. (1966). Small Differences Between Prime Numbers. *Proc. R. Soc. Lond. A,* 293(1432), 1-18.

Brent, Richard P. (1990). Primality Testing and Integer Factorisation, Australian Academy of Science Annual General Meeting Symposium on the Role of Mathematics in Science, Canberra Proceedings, 14-26.

Couveignes, Jean-Marc., Tony, Ezome. and Reynald, Lercier. (2012). A Faster Pseudo-Primality Test. *Rendiconti del Circolo Matematico di Palermo,* 61(2), 261-278.

Crandall, Richard. and Carl, B. Pomerance. (2006). *Prime Numbers: A Computational Perspective*, 182. Springer Science & Business Media.

Dixon, John D. (1984). Factorization and Primality Tests. *The American Mathematical Monthly,* 91(6), 333-352.

Gordon, Daniel, M. (1998). A Survey of Fast Exponentiation Methods. *J. Algorithm,* 27(1), 129-146.

Gunasekara, ARC De Vas, A.A.C.A. Jayathilake. and Perera, A.A.I. (2015). Survey on Prime Numbers, Elixir Appl. Math. 88, 36296-36301.

Heath-Brown, D.R. (1982). Prime Numbers in Short Intervals and a Generalized Vaughan Identity. *Canadian Journal of Mathematics,* 34(6), 1365-1377.

Hua, Luogeng. (2009). *Additive Theory of Prime Numbers*, 13. American Mathematical Soc. Translations of Mathematical Monographs, 13, 190p.

Hussein, Nidal Hassan., Ahmed Khalid, and Khalid Khanfar. (2016). A Survey of Cryptography Cloud Storage Techniques. Google Scholar.

Ingham, Albert Edward, and Albert, Edward, Ingham. (1990). *The Distribution of Prime Numbers*. No. 30. Cambridge University Press.

Kandola, Shelley. (2013). A Survey of Cryptographic Algorithms. Diss. St. Lawrence University.

Lenstra, Arjen, K. (1990). Primality Testing. Cryptology and Computational Number Theory, *Proc. Symp. Appl. Math.*, 42.

Lenstra, H.W. (1981). Primality Testing Algorithms [after Adleman, Rumely and Williams]. *Séminaire Bourbaki vol. 1980/81 Exposés* 561-578. Springer, Berlin, Heidelberg, 243-257.

Morain, François. (1993). Pseudoprimes: A Survey of Recent Results. *Eurocode'92*, 207-215. Springer, Vienna.

Pomerance, Carl. (2010). Primality Testing: Variations on a Theme of Lucas. *Congr. Numer,* 201, 301-312.

Šleževiciene, R., Steuding, J. and Turskiene, S. (2004). Recent Breakthrough in Primality Testing. *Nonlinear Analysis,* 9(2), 171-184.

Wells, David, G. (2005), *Prime numbers*. John Wiley & Sons, Inc., Hoboken, New Jersey.

Williams, H.C. (1982). The Influence of Computers in the Development of Number Theory. *Computers & Mathematics with Applications,* 8(2), 75-93.

Williams, Hugh, C. (1984). An Overview of Factoring. *Advances in Cryptology*. Springer, Boston, MA.

Cite this article as: Sumit Tiwari and Atin Kushwaha (2022). A Theoretical Approach on Deterministic and Probabilistic Prime Numbers. *International Journal of Pure and Applied Mathematics Research*, 2(1), 65-73. doi: 10.51483/IJPAMR.2.1.2022.65-73.