On Prime Numbers and Related Applications

V Yegnanarayanan, Veena Narayanan, R Srikanth

***Abstract*: In this paper we probed some interesting aspects of primorial and factorial primes. We did some numerical analysis about the distribution of prime numbers and tabulated our findings. Also, we pointed out certain interesting facts about the utility value of the study of prime numbers and their distributions in control engineering and Brain networks.**

***Keywords*: Factorial primes, Primorial primes, Prime numbers.**

I. INTRODUCTION

The irregular distribution of prime numbers makes it difficult for us to presume and discover. Euclid about 2300 years before established that primes are infinitely many. Till date we are not aware of a formula for finding the nth prime. It appears as if they are randomly embedded in N and may be because of this that sequences of primes do not tend to emanate from naturally happening processes. We constantly use computer encryption whenever we communicate our credit card information to Amazon or logging into our bank account or posting an encrypted email. It simply implies that we are using prime numbers and rely on their properties for protection of life in this cyber-age. Carl Sagan in his novel "Contact" remarked that prime numbers are cool. He further said in that book that aliens prefer to encode their message as long string of prime numbers. Many of the cryptographic algorithms depend on finding large prime numbers. So, if one did not perform the primality testing with a proper prime gap, then the algorithm itself would consume a very long time to run. Thus, one of the interesting questions arising in the study of prime numbers is the distance between two successive primes. According to Grandville, understanding both the small and large prime gaps is extremely difficult and hence would not be answered until another era.

Lately problems in number theory are handled with the math software tools such as maple or MATLAB. These tools processes complex computations with ease reducing voluminous labor. It is incredible to note that Goldbach's conjecture was found to be true through numerical techniques for every number that is congruent to zero (mode 2) but less than or equal to 4×10^{18}.

Revised Manuscript Received on October 30, 2019.
***** Correspondence Author

Veena Narayanan*, Department of Mathematics, SASTRA Deemed University, Thanjavur, India. Email: veenanarayanan@sastra.ac.in

V Yegnanarayanan, Department of Mathematics, SASTRA Deemed University, Thanjavur, India. Email: prof.yegna@gmail.com

R Srikanth, TATA Realty-SASTRA Srinivasa Ramanujan Research chair for Number theory, SASTRA Deemed University, Thanjavur, India. Email: srikanth@maths.sastra.edu

Our motivating factor for this work stems from the classic result of called Prime Number Theorem which beautifully models the statistical behavioral pattern of huge primes viz., chance for an arbitrarily picked $n\epsilon N$ to be a prime number is inverse in proportion to $\log(n)$.

II. RESULTS AND DISCUSSIONS

A. Discussion on Primorial and Factorial Primes

Our journey is driven by fascinating characteristics of primordial primes and factorial primes. A primordial function denoted $P\#$ is the product of all primes till P and includes P. The factorial function is $n! = \prod_{i=1}^{n} i$. A natural curiosity pushes us to probe large primes. In order to do this, we need to get an idea by analyzing numbers such as $n!+1, n!-1, P\#+1, P\#-1$. As these numbers have large factors it is quite evident that their density of primes is more than the average. The following facts are well known. One can also see [1]-[4] for more.

(a) The density of primes close to M is ${}^{1}/_{\log M}$.

(b) $N! \approx \left(\frac{N}{e}\right)^{N}$

(c) If $p\epsilon\left(N, \sqrt{N!+1}\right), p$ prime and $(N!+1) \not\equiv 0\ (mod\ p)$, then $N!+1$ is a prime.

The task of determination of huge primes comprises two distinct steps. The first step is to determine the chance of being a prime and the second step is testing for the primality. A number A is declared to have more chance of being a prime if $(c^{A-1}-1) \equiv 0(mod\ A)$. Here the option for c is not that pertinent except in typical situations where c is restricted from assuming certain forbidden values. It has already been estimated that the mathematical expectation of the number of primes from $K_1\ to\ K_2$ is $I = \int_{K_1}^{K_2} \frac{2dK}{K} = 2\log(\frac{K_2}{K_1})$ and hence it takes significantly longer time to determine the succeeding factorial prime. Next, about the testing of primality, if a huge integer with more than 10^5 digits has higher chance of being a prime then in reality it mostly turns out to be so. A nice reference for practical tests for primality of huge numbers with 10^5 or above digits is [5]. Starting with 2, as first prime number, it is customary to let $\pi(x)$ as number of prime less than or equal to x; $\vartheta(x)$ as the logarithm of product of all primes less than or equal to x, $\Psi(x)$ as the logarithm of the lcm of all positive integers less than or equal to x; Also we let $\pi(x) = \vartheta(x) = \Psi(x) = 0\ if\ x < 2\ and\ x\epsilon R$. In [6] the authors have obtained nice upper and lower bounds for $\pi(x), \vartheta(x)\ and\ \Psi(x)$. A natural approach to determine an approximation for the summation $\sum f(p)$ p ≤ x is to let it as equal to $\int_2^x \frac{f(y)dy}{\log y}$.

In view of this, $\pi(x) and\, \vartheta(x)$ becomes $\int_2^x \frac{dy}{\log y}$ and $\int_2^x dy$ which is close to x. It has been universally agreed that the following numerical approximations or estimations are accurate and valid for almost all values. That is, $x/\log x \left(1+\frac{1}{2\log x}\right) < \pi(x) < \frac{x}{\log x}(1+\frac{3}{2\log x})$ where $x \geq 59$ for lower inequality and $x > 1$ for upper inequality. $x/\left(\log x - \frac{1}{2}\right) < \pi(x) < x/\left(\log x - \frac{3}{2}\right)$ for $x \geq 67$ for the lower inequality and $x > e^{1.5} = 4.48$ for the upper inequality. $x/\log x < \pi(x) < 1.25506\ x/\log x$ where $x \geq 17$ for lower inequality and $x > 1$ for the upper inequality. $x\left(1 - 1/(2\log x)\right) < \vartheta(x) < x\left(1 + 1/(2\log x)\right)$ where $x \geq 563$ for the lower inequality and $x > 1$ for the upper inequality. $\{1 -$ *logxe−logxRx<ϑ(x)≤Ψ(x)* and $\vartheta(x) \leq \Psi(x) < \left\{1 + \left(\sqrt{\log x}\right)e^{-\sqrt{\frac{\log x}{R}}}\right\}x$ where $R = 515/(\sqrt{546} - \sqrt{322}) \approx 217.51631$ and $x \geq 2$ for lower inequality and $x > 1$ for the upper inequality.

B. On Distribution of Primes

It is a fact that till date there are 183 different proofs for the Euclid's observation that primes are infinitely many. So by beginning with $p_1 = 2,$ if we presume that $p_1, p_2, \ldots, p_k$ are defined then by selecting a prime p_{k+1}, one can continue the sequence for which N $\prod_{j=1}^{k} p_j + 1 \equiv 0\ (mod\ p_{k+1})$. Clearly such a sequence of selection $\{p_j\}$ is not unique as there are many options for p_{k+1} to keep the above relation intact. Mullin [7] proposed two canonical options namely the least p_{k+1} and the greatest p_{k+1}. The former resulted in a sequence $2,3,7,43,13,53,5,6221671,38709183810571,$ $139,2081,11,17,5471,\ldots$ [8] called first EM-sequence and the latter in 2,3,7,43,139,50207,340999, 2365347734339, … [9] called the second EM-sequence. Mullin then asked whether these two sequences include in it every prime. In [10] it was conjectured relaying on stochastic arguments that the second EM sequence would in all possibility could exhaust all primes by having them in their length but till date not much is known about the first EM sequence. Later the second EM sequence was probed further in [11] and the authors reported that all of $5,11,13,17,19,23,29,31,37,41$ and 47 are missing and they conjectured that infinitely many primes do not occur in the second EM sequence. The authors in [12] confirmed this conjecture in positive. Understandably they used quadratic reciprocity for the Jacobi symbol and made a good use of the works of Burgess on short character sums' upper bound.

In this article, we are discussing about the primes of the form $y = 2\prod_{i=1}^{k} x_i + 1;\ x_i \in P - \{2\};\ x_i's$ are distinct. It is to be noted that if these $x_i's$ are consecutive primes, then we obtain primorial primes.

C. Numerical Analysis on Distribution on Primes

Here we provide a heuristic estimate for the primes of the form $y = 2\prod_{i=1}^{k} x_i + 1;\ x_i \in P - \{2\};\ x_i's$ are distinct. If $\pi(n) = \#\{k \leq n : k \text{ is prime}\}$ defines the number of primes not exceeding a fixed real number n, then the Prime Number Theorem (PNT) states that $\pi(n) \sim \frac{n}{\ln n}$ where ln is the natural logarithm. The Table I interprets this.

Table-I: Calculation of $\pi(n) \sim \frac{n}{\ln n}$

n	$\pi(n)$	$\frac{n}{\ln n}$
10	4	4.3429
50	15	12.7811
100	25	21.7142
500	95	80.4559
1000	168	144.7648
5000	669	587.0478
10000	1229	1085.7362
50000	5133	4621.16678
100000	9592	8685.88964

Now define $\pi^*(n) = \#\{y \leq n: y \text{ is prime}\}$ where $y = 2x_1x_2 \cdots x_k + 1;\ x_i \in P - \{2\}$ are distinct. Then the Table II gives the ratio of $\pi^*(n)$ to $\pi(n)$.

Table-II: . Ratio of π*(n) to π (n)

n	π(n)	π^*(n)	Ratio
10^2	25	5	0.2
10^3	168	36	0.21428
10^4	1229	261	0.21236

From Table II it is clear that $\pi^*(n) \sim \alpha\, \pi(n)$ where $\alpha \approx 0.21$. Then by PNT we can say that $\pi^*(n) \sim \alpha \frac{n}{\ln n}$ where $\alpha \approx 0.21$. Thus, we can enhance the approximation for the property of being y to be prime as ln n. The Table III presents a comparison of the actual number to the estimated number of primes we considered. The Fig.1. represents the plot for Table III.

Table-III: Comparison of Estimates

n	Actual number	Expected number	Ratio
10^2	5	4.56	1.096
10^3	36	30.4006	1.1841
10^4	261	228.004	1.1447

Retrieval Number: L36521081219/2019©BEIESP
DOI: 10.35940/ijitee.L3652.1081219
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

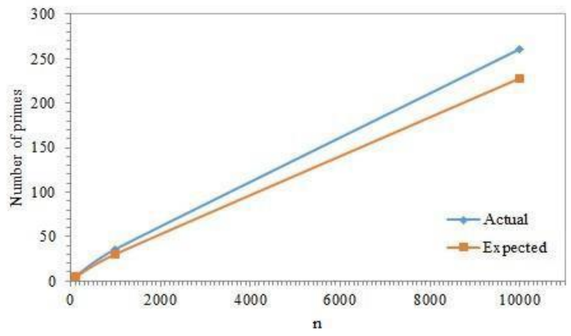

Fig.1. Variation of Actual to Expected Number of Primes of the particular case

It is noted that the heuristic estimates for the Primorial and Factorial primes were determined by Caldwell and Gallot [13]. According to them, both the Primorial and Factorial primes have the same heuristic estimate given by the formula $e^{\gamma}\ln(N)$ where N is a fixed real number. We compare these ratios with the ratio of present study in Table IV.

Table-IV: Comparison with Primorial and Factorial primes

n	Present	Primorial Estimate [7]	Factorial Estimate [7]
10	0	4.1	4.1
10^2	4.56	8.2	8.2
10^3	30.4006	12.3	12.3
10^4	228.004	16.4	16.4

III. APPLICATIONS

A system that deploys measurements to self-evaluate its behavior for the purpose of better imminent behavior is called a feedback and control system (FCS). According to [14] FCS can be described by differential equations and prime numbers are some type of fcs. This thought process has occurred to them on seeing the random distribution of prime numbers along the integer number line. Much earlier to this observation Gauss remarked that the density of primes is inversely proportional to $\ln x$. Using Gauss's remark, the function $\pi(x)$ was coined to denote the number of primes not exceeding x. To comprehend FCS mechanism of primes, it was first observed that a presence of a large number of primes in one given interval affects that much presence in a subsequent larger interval while its meagre presence in a given interval boosts its chance of presence in larger numbers in higher intervals. So, by following Eratosthenes sieve process one can see early that the removal process of primes alters the density by a factor of $1 - 1/p$. In [14] the authors nicely derived the following differential equation that models the density of primes at x.

Suppose that $g(x)$ represents a differentiable function that roughly describes density of primes in the nearest neighborhood of x. Then the change in density on an interval with end points x^2 and $(x + dx)^2$ is $g((x + dx)^2) - g(x^2)$. Note that every prime in $(x, x + dx)$ changes the density on $(x^2, (x + dx)^2)$ by a factor of $1 - 1/x$. So, every prime remove $g(x^2)/x$ from the density. As there are $g(x)dx$ primes in $(x, x + dx)$, a first approximation in the density variation on $(x^2, (x + dx)^2)$ is $g((x + dx)^2) - g(x^2) \cong \frac{-g(x^2)g(x)}{x}dx$. Another estimate of variation in density comes with the help of derivatives namely, $g((x + dx)^2) - g(x^2) \cong g'(x^2)2xdx$. So $g'(x^2) = -g(x^2)g(x)/2x^2$. A change of variable from x^2 *to* x yields $g'(x) = \frac{-g(x)g(\sqrt{x})}{2x}$.

The randomness in prime number distribution can be stochastic or deterministic. As the prime numbers' distribution behaves Poissonian-like there is better chance that they are stochastically distributed [15]. The authors in [16] however presume that prime numbers may be eigenvalues of a quantum system. A primary reason for attempting to decipher the pattern of distribution of prime numbers is that one can compare them with the hidden or known patterns in the computational nature of brains, where the natural numbers have a significant role. The randomness of neuron signals is similar to that of prime numbers.

IV. OPEN PROBLEMS

In this section we point out some open problems existing in the study of prime numbers in applied areas like control systems and bio-networks.

(i) Prove or Disprove the theoretical nature of the prime numbers.

(ii) Test whether any intermittent designs are there in the sequence of prime numbers.

(iii) Is it possible to relate patterns detected in neuron signals with the prime number pattern to describe the computational device of the brains.

(iv) How to describe the source of interspike breaks anomaly to provide for the sequential components of the neuronal code

(v) How to compare the impulsive movement of the hippocampal singular neurons with the randomness of the prime numbers.

V. CONCLUSIONS

In the present study we discussed on prime numbers, their distribution and some applications. Also, we introduced some numerical analysis on primes of the form $= 2\prod_{i=1}^{k} x_i + 1$; $xi \in P-2$; $xi's$ are distinct. We compared our findings with primorial as well as factorial primes. Then we discussed certain interesting application regarding the effectiveness of primes and their distributions in control system and Bio Engineering. Also, we pointed out some open problems in engineering fields other than cyber security and cryptography.

ACKNOWLEDGMENT

The authors gratefully acknowledge Tata Realty-SASTRA Srinivasa Ramanujan Research Chair Grant for funding this research work.

REFERENCES

1. A Borning, "Some results for k! + 1 and 2 × 3 × 5 × · · · × P + 1" , *Mathematics of Computation*, 1972, pp.567–570.
2. M. Templer. "On the Primality of k! + 1 and 2 × 3 × 5 × · · · ×P+ 1", *Mathematics of Computation*. 1980, vol. 34, pp.303–304.

3. J.P. Buhler, R. E. Candall, and M.A. Penk. "Primes of the form M ! + 1 and 2 × 3 × 5 × · · · × P + 1", *Mathematics of Computation*, 1982, vol. 38, pp. 639–643.
4. Ondrejka, "Ten extraordinary primes", *Journal of Recreational Mathematics*, 1985-1986, vol. 18(2)., pp.87-92.
5. J. Brillhard, D. H. Lehmer. and J .L .Selfridge., "New primality criteria and factorizations of 2n + 1", *Mathematics of Computation*, 1975, vol. 29 , pp. 620–647.
6. B. J. Rosser and L. Schoenfeld., "Approximate formulas for some functions of prime numbers", *Illinois.Journal of Mathematics*, 1962, vol. 6, pp. 64-94
7. A. A. Mullin., "Recursive function theory (a modern look at a Euclidean idea)", *Bulletin of American Mathematical Society*, 1963, vol. 69 , pp. 737.
8. H. Dubner., "Factorial and primorial primes", Journal of Recreational mathematics, 1987, vol. 19(3), pp. 197–203
9. N.J.A. Sloane., "The On-Line Encyclopedia of Integer Sequences", published electronically at http:// oeis.org.
10. D. Shanks, "Euclid's primes", *Bull. Inst. Combin. Appl*., 1991, vol. 1, pp. 33–36
11. C. D. Cox, and A. J. Van der Poorten, "On a sequence of prime numbers", *Journal of Australian Mathematical Society*, 1968, vol. 8, pp. 571– 574.
12. A. Booker, "On Mullin's second sequence of primes", *Integers*, 2012, 12A(2012), available at http://www. integers-ejcnt.org/vol12a.html.
13. C.K. Caldwell. and Y. Gallot., "On the primality of n! ±1 and 2×3×5×· · ·×P ±1", *Mathematics of Computation*, 2002, vol. 71(237), pp. 441–448.
14. H. Susan. Marshall and Donald. R.Smith, "Feedback, Control and the Distribution of Prime numbers", *Math.Mag*, 2013, vol. 86, pp.183-203. doi:10.4169/math.mag.86.3.189
15. K. Soundararajan. "The distribution of prime numbers", *NATO Science Series II: Mathematics, Physics and Chemistry*, 2007, vol.237, 59-83.26.
16. T. Timberlake. and J. Tucker., "Is there quantum chaos in the prime numbers*?", Bulletin of the American Physical Society*, 2007, vol.52, pp. 35.

AUTHORS PROFILE

Veena Narayanan is a research student in SASTRA. She enrolled for Ph.D. in 2017. Her area of research is Number Theory. She completed her schoolings in Kerala. She had secured third rank in Bachelor degree and First rank in Master degree under Calicut University, Kerala. She has one year of teaching experience and two years of research experience. Her research is funded by TATA Realty SASTRA Srinivasa Ramanujan Research chair grant.

V.Yegnanarayanan obtained his Full Time PhD in Mathematics from Annamalai University in Nov 1996. He has 31 years of total experience in which 16 years as Professor & Dean/HOD. He has also worked as a Visiting Scientist on lien in TIFR and IMSC. He has authored 164 research papers and guided 6 students to Ph.D. degree. He has delivered a number of invited talks, organized funded conferences, FDP etc., did a lot of review work for MR, zbMATH and reputed journals, completed research projects funded by NBHM-GOI, won Sentinel of Science Award from Publons. TN State (Periyar) University has recognized his qualifications and experience for the post of Principal in 2009.

R Srikanth is a chair professor for Number Theory under TATA Realty-SASTRA Srinivasa Ramanujan Research chair. His area of specialization is Number Theory and allied areas. He had a lot of experience in teaching as well as in Research for many years both in core subject and applied area. He received his Doctoral degree (Mathematics, Number theory) from Bharathidasan University, Trichy in 2006. He has completed one DST project on "Optimal Rehabilitation and Expansion of Water Distribution Networks" from 2008 to 2010 and a DRDO sanctioned project on "A Novel methodology for the identification of newer elliptic curve that are band suited to cryptosystem" from2013-2015.