Numerical Model to Estimate higher order safe prime number

Saad Qasim Abbas

Department of Mathematics - Diyala University
saabqasim75@gmail.com

Abstract

This paper is devoted to present a numerical model to estimate the density of higher-order prime in a set of integers v .This model is examined along this paper and the results are listed out ,and standard primarily tests are deployed to confirm the result of the model presented in this paper .Safe prime has been the essential concern when developing public key cryptographic applications, the density of safe primes is vital parameter to select a proper range on integers .The result along this paper has been compared with other mathematical approaches to evaluate the safe prime density .A table of the comparisons shows the performance of this numerical model

Keywords: Numerical model, density of higher-order prime number.

النموذج الرياضي لتخمين العدد الأولي الأمن ذو الرتبة العالية

سعد قاسم عباس

قسم الرياضيات - جامعة ديالى

saabqasim75@gmail.com

الخلاصة

كرّس هذا البحث من اجل تَقديم نموذج عددي لتَخمين كثافةِ العدد الاولي الامن ذي الرتبة العالية ضمن مجموعة من الاعداد الصحيحة v , لقد تم اختبار هذا الموديل وتم عرض النتائج, وتم استخدام معاير أولية لتَأكيد نتيجةِ النموذجِ .كثافةِ العدد الاولي الامن اعتمدة بصورة اساسية عندما تم تُطوّيرُ التطبيقاتَ المشفّرةَ الرئيسيةَ العامّةَ ،حيث يعتبر كمعيار حيوي لمجموعة من الأعداد الصحيحة , لقد تم مقارنة النتائج لهذا البحث مع نماذج رياضية مختلفة لتحديد الكثافة من خلال جدول يوضح اداء هذه الطريقة .

الكلمات المفتاحية : النموذج العددي، العدد الأولي الأمن ذو الرتبة العالية.

1- Introduction

The two most important characteristics of the sequence of primes is that, there are many of them but that their density is rather slim. Euclid's showed that there are infinitely many primes [1]; in fact there are infinitely many in any nontrivial arithmetic sequence of integers, this fact was proved by Dirichlet and is known as Dirichlet's theorem [2]. If x is a natural number and $\pi(x)$ represents the number of primes less than or equal to x, then this function behaves like the function $\frac{x}{\ln x}$ This result is known as the prime number theorem [see for example reference 3], which addresses the global smoothness of the counting function $\pi(x)$ providing the number of primes less or equal to integer $x$was the first hint of such regularity.

The prime number theorem was originally conjectured by both Guass and Legendre [4], although Euler also surmised the result [4]. The attempted proof of the prime number theorem was begin by Chebychev in 1848. He proved that there exist constants A_1 and A_2 with .922 < A_1 <1 and 1< A_2 < 1.105 such that

$$A_1 < \frac{\pi(x)}{x/\ln x} < A_2 \qquad (1)$$

Riemann in 1859 [7] attempted to give a complete proof using complex analysis. His work considered the beginnings of modern analytic number theory. This refers to the use of analytic methods, especially complex analysis, in the study of number theory.

Legendre [4] published a bit earlier than Gauss looking at the list of primes up to 1,000,000, came up with a the formula:

$$\pi(x) \approx \frac{x}{\ln(x) - 1.08366} \qquad (2)$$

Gauss looked at the list less than 3,000,000 and noticed that the prime number function is given by the function *Li(x)* which was defined by the integral

$$Li(x) = \int_2^x \frac{1}{\ln t} dt. \qquad (3)$$

Gauss's observation was then that

$$\pi(x) = Li(x) \qquad (4) .$$

If we integration Equation (3) by parts is used on the integral defining *Li(x)* and we take the limit as $x \to \infty$, it is clear that this integral is **Asymptotically** means goes to zero.

Finally In 1896, Hadmard and independently, C. de la Vallee Poussin proved the prime number theorem [4].Their proofs relied heavily on complex analysis. It was considered for a long time that the prime number theorem was at least as complicated as the theory of complex variables. Most mathematicians doubted that a proof that did not heavily rely on the theory of analytic functions could be found. However, in 1949 Selberg [5] and later Erdfe came up with an elementary proof of the prime number theorem. This proof is actually harder than the analytic proof but is elementary in that it doesn't use any complex analysis.

2- Cryptography and prime number [8]

Cryptography is the study of the methods that allow the secure transmission of information; two main types of cryptography exist:

a) ***Secret key:*** The classical method, used since ancient Rome, it is useful only when the number of users is small, since its correct working requires each user to agree on - and exchange secret key with - every other user prior to use;
b) ***Public key:*** the modern method, it allows secure communication even when the number of users is high, since it does not require a prior exchange of secret keys. It was first proposed by Diffie and Hellman in 1976.

At first sight, public key cryptography seems impossible. In order to persuade you of the opposite, we propose the classical example of the double lock. Suppose that there are two users ***A*** and ***B*** and that ***A*** wants to send a secret message to ***B***;

1) ***A*** puts the message in a box, locks it with her lock ***LA*** (Only ***A*** has a key to this lock) and then sends it to ***B***.
2) ***B*** receives the box locked with lock ***LA*** and adds her own lock ***LB*** (only B has a key to this lock) and sends everything back to ***A;***
3) ***A*** receives the box with double lock, removes lock ***LA*** and re-sends the box to ***B***;
4) At this point, having received the box, ***B*** can remove the lock ***LB*** and read ***A's*** message.

The security of this method lies in the fact that the keys to open the two locks are known only to the respective owners (who have not agreed on and exchanged keys prior to the transaction). One of the "mathematical versions" of this idea is ***R.S.A.*** public key cryptography, proposed by Rivest, Shamir and Adleman in 1978 ,which depends on necessity to build large primes to send the massage and this operation is computationally fast and factories large natural numbers obtained as product of two primes to decode the massage such operation is Computationally "slow" .this difference in the speed of execution of operations

,to determine large primes on the one hand and to factories large numbers on the other , guarantees the security of the method, at least for a sufficiently long period of time. For instance at the current stele of technology, a natural number of 140 digits in base 10 can be produced through "multiplication of two random primes in a few seconds on a typical normal computer available. Yet, the factorization operation of such 140-digit natural number would require about month when employing several supercomputers working in parallel. Increasing the number of digits further increases the security of the system: it is currently recommended that numbers of at least 220 digits in base 10 be utilized.

3- Chebychev’s estimation and prime number

Where The prime number function $\pi(x)$ and the prime number theorem answer the basic questions concerning the density of primes. A related question concerns the function

$$p(n) = p_n \qquad (5).$$

where p_n is the nth prime. That is the question whether there is a closed-form function that estimates the *nth* prime. The answer to this is yes and turns out to be equivalent to the prime number theorem. We state it below.

Theorem 3.1 *The nth prime p_n is given asymptotically by*

$$p_n \sim n ln(n). \qquad (6)$$

Proof : From the prime number theorem we have that $\pi(x) \sim x/\ln x$, Let

$$y = x/\ln x, \qquad (7)$$

which implies that

$$In\, y \;=\; In\, x - \; In\, In\, x. \qquad (8)$$

But In $In\, x$ is asymptotically small compared to $In\, x$, and hence

$$In\, y \sim In\, x. \qquad (9)$$

Now

$$x \;=\; y\, In\, x \sim y\, In\, y. \qquad (10)$$

This shows that the inverse function to $x/\ln x$ is asymptotically $x\ /In\ x$. But by the prime number theorem this is asymptotically the inverse function of $\pi(x)$.

Notice that this Theorem. have recovered the prime number theorem.

3.1 Chebychev Estimate

The first significant progress in developing a proof of the prime number theorem was obtained by Chebychev in 1848 ,he proved that the functions $\pi(\mathrm{x})$ and $\mathrm{x}\ /\mathrm{In}\ \mathrm{x}$ are of the same order of magnitude, a concept we will explain in detail below, and that if $\lim_{n\to\infty}\frac{\pi(x)}{x/\ln x}$ existed then the limit would have to be 1. At first glance it appeared that he was quite close to a proof of the prime number theorem.

However, another fifty years and the development of some completely new ideas from complex analysis to actually accomplish this. A proof, along the lines of Chebychev 's methods, without recourse to complex analysis, would not be done until the work of Selberg and ErdOs in the late 1940s .

Chebychev proved the following result, now known as **Chebychev's estimate.**

Theorem 3.1. There exist positive constants A_1 and A_2 such that

$$A_1\frac{x}{\ln x} < \pi(x) < A_2\frac{x}{\ln x}, \qquad (11)$$

for all x > 2.

Proof see [4].

This theorem says that the primes become relatively scarcer as *x* gets larger. In probabilistic terms it says that the probability of randomly choosing a prime less than or equal to *x* goes to zero as *x* goes to infinity. The more interest in this probabilistic sense that the probability of randomly choosing a prime is relatively not that small. For any x the probability of randomly choosing a prime less than *x* is $\pi(x)/x$ for large x this Approximately equal to $1/\ln(x)$ even for very large real numbers *x*, this is not that small. The number e^{200} has 86 decimal digits, yet the probability of randomly choosing a prime less than this value is about .005. This argument shows that the primes, although scarce, are still rather dense in the integers. As we have already remarked, the primes are asymptotically denser in the sequence of squares (1, 4, 9, 16, ...}. This relatively high probability of locating a prime will play a role in cryptography.

4- The prime-counting function in terms of the logarithmic integral and Approximations for the nth prime number

The German Mathematician Johann Carl Friedrich Gauss (30 April 1777 - 23 February 1855) conjecture that an even better approximation to $\pi(x)$ is given by the logarithmic integral function $\mathrm{Li}(\pi)$, the discrete version defined by

$$\mathrm{Li}(x) \cong \frac{x}{\ln x} \sum_{k=0}^{\infty} \frac{k!}{(\ln x)^k}. \qquad (12)$$

This integral is strongly suggestive of the notion that the 'density' of primes around x should be $1/\ln x$. the logarithmic integral function or integral logarithm $Li(x)$ is a Special function. This function is related to the logarithm by the asymptotic expansion

$$\mathrm{Li}(x) \approx \frac{x}{\ln x} \sum_{k=0}^{\infty} \frac{k!}{(\ln x)^k} = 1 + \frac{x}{(\ln x)^2} + \frac{2x}{(\ln x)^3} + \cdots, \qquad (13)$$

So, the prime number theorem can also be written as $\pi(x) \sim \mathrm{Li}(x)$. In the table below we compare the exact values of $\pi(x)$ to legendre formula and gauss function $Li(x)$ and $\pi(x)$ from the prime number thorem which show that $\pi(x) \approx x/\ln(x)$,we show the legender formula is true when replace 1.08366 with 1 ,and the difference is very small.

Table 4.1 the compared values density of prime number calculated in different whys

x	$\pi(x)$	$\pi(x)-\frac{x}{\ln(x)-1}$	$\pi(x)-\frac{x}{\ln(x)-1.08366}$	$\pi(x)-\int_2^x \frac{1}{\ln t}dt$	$\pi(x)-\frac{x}{\ln(x)}\sum_{k=0}^{\infty}\frac{k!}{(\ln x)^k}$	$\pi(x)-\frac{x}{\ln(x)-1}$
10	4	-3.4294e-	-4.2039e+000	2.2	-4.490	6.5706e-001
10	25	3.2853e-	-3.3969e+000	5.1	-	4.2853e+000
10	168	2.32356+0	-3.70056+000	10	-	2.4235e+001
10	1229	1.4326e+0	-1.514764000	17	-	1.4426e+002
10	9592	9.0611e40	3.5970e4000	38	-	9.0711e+002
10	78498	6.1156e-	-4.5178e+001	130	-	6.1166e+003
10	664579	4.4158e-	-5.6070e+002	339	-	4.4159e+004
10	5761455	3.3277e-	-6.5487e+003	754	-	3.3277e+005
10	50847534	2.5926e+0	-6.9985e+004	1701	-2.728	2.5926e+006

10	455052511	2.07586+0	-6.9049eHX)5	3104	-	2.0758e+007
10	4118054813	1.6992e+0	-6.5451e+006	11588	-	1.6992e+008
10	37607912018	1.4167e-	-6.0615e+007	38263	-	1.4167e+009
10	346065536839	1.1993e+0	-5.5556e+008	108971	-	1.1993e+010
10	3204941750802	1.0284e+0	-5.0703e+009	314890	-	1.0284e+011
10	29844570422669	8.9160e-	-4.6224e+010	1052619	-	8.9160e+011
10	279238341033925	7.8043e+0	-4.2169e4011	3214632	-	7.8043e+012
10	2623557157654233	6.8884e-	-3.8534e+012	7956589	-	6.8884e+013
10	2473995428774086	6.1248e-	-3.5290eH)13	21949555	2.0504e+01	6.1248e+014
10	2340576672763446	5.4816e-	-3.2398e+014	99877775	2.3406e+01	5.4816e+015
10	2220819602560918	4.9347e+0	-2.9819e+015	22274464	2.2208e+01	4.9347e+016
10	2112726948601873	4.4658e+0	-2.7517e4016	59739425	2.1127e+01	4.4658e+017
10	2014672866893159	-	-2.0170e+020	19323552	2.4740e+01	-1.9738e+020
10	1925320391606803	-	-1.9274e+021	72501862	2.3406e+01	-1.88806+021

5-proposed numerical model for prime density estimation:

Several mathematical insights regarding Benford's law have also been put forward so far and proved a central Limit _like theorem [5] which states that random entries picked from random distributions form a sequence whose first- digit distribution tends towards Benford's Law explaining thereby its ubiquity practically, this law has for a long time been the only distribution that could explain the presence of skewed first-digital frequencies in generic of datasets Recently proposed a generalization of Benford's law based on multiplicative processes. It is well known that a stochastic process with probability density $\frac{1}{x}$ generates data that are Benford; therefore, Series generated by power-Law distributions $p(x) \sim x^{-\propto}$,with $\propto \neq 1$,would have a first – digit distribution the follows a so-called GBL

$$p(d) \; = c\int_{d}^{d+1} x^{-\propto}\, dx = \frac{1}{10^{1-\propto}-1}\left[(d+1)^{1-\propto} - d^{1-\propto}\right] \qquad (14)$$

Where the prefactor is fixed for normalization to hold and $\propto$ is the expond of the original power-Low distribution (observe that for $\propto = 1$ the GBL reduces to the benford low , while for $\propto = 0$ it reduces to the unigorm distribution .

5-1 The first-digit frequencies of prime numbers:

Although Diaconis showed that the leading digit of primes distributes uniformly in the infinite Limit [6] , there exists a clear bias from uniformity for finite set.given an interval $[1, \mathrm{N}]$ there exists a particular value $\propto (\mathrm{N})$ for which a GBL fits with extremely goad accuracy the first – digit distribution of the primes appearing in that interval observe of this point that the functional dependency of$\propto$ is only in the interval’s .

Upper bound ; once this bound is fixed , $\propto$ is constant in that intervals Interestingly, the value of the fitting parameter $\propto$ decrease as the intervals upper bound, hence the number of primes , Increases in figure 5.1

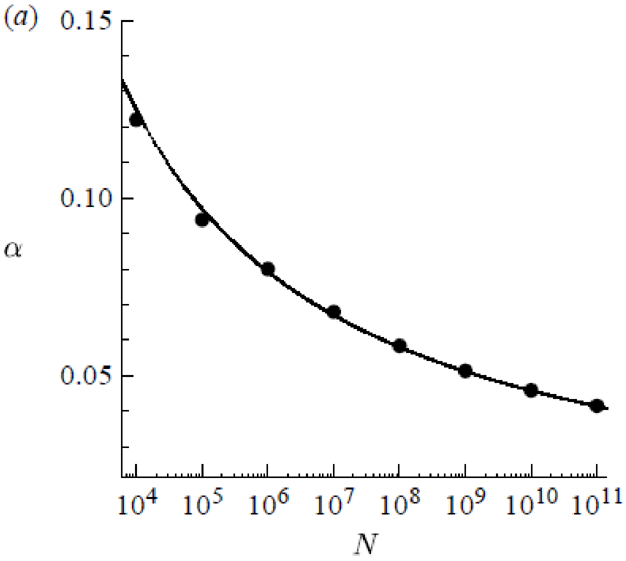

Figure 5.1. Size-dependent parameter α. circles represent the exponent $\alpha(N)$

We have plotted this size dependence , showing that a functional relation between $\propto$ and N seems to take place

$$\propto (N) = \frac{1}{logN - a} \qquad (15)$$

where $a = 1.1 \pm 0.1$ is the best fit .Note that $\lim_{N\to\propto} \propto(N) = 0$ and this size dependent GBL reduces asymptotically to the uniform distribution. Which is consistent with previous theory . Despite the Local randomness of the prime number sequence.

The prime counting function $\pi(N)$ provides the number of primes in the interval $[1, N]$and up to normalization, stands as the cumulative distribution function of prime. While $\pi(N)$is a stepped function ,a nice asymptotic approximation is the offset logarithmic integral

$$\pi(N) \sim \int_Z^N \frac{1}{logx} dx = li(N) \tag{16}$$

We can interpret $\frac{1}{\log x}$ as an average prime density and Lower bound of the interval $[1, N]$.

5-2 The primes counting function $\boldsymbol{L(N)}$:

Suppose that a given sequence has a power-Low-Like density $x^{-\propto}$(and whose first significative digits are consequently GBL). One can derive from this latter density a counting function $L(N)$ that provides the number of elements of the sequence appearing in the interval $[1, N]$.

A first option is to assume a Local density of the shape $x^{-\propto(x)}$ such that $L(N) \sim \int_Z^N x^{-\propto(x)}\, dx$.Note that this option implicitly assumes that $\propto$ varies smoothly in $[1, N]$,which is not the case in the light of the numerical relation

$$\propto (N) = \frac{1}{\log N - a} \tag{17}$$

which implies that the functional dependency of $\propto$ is only which respect to the upper bound value of the interval. Indeed $x^{-\propto(x)}$ is not agood approximation to $\frac{1}{\ln x}$ for any given interval. This drawback can be over come defining $L(N)$as follous:

$$L(N) = e\propto(N) \int_Z^N x^{-\propto(N)}\, dx \tag{18}$$

Where the prefactor is fixed for $\mathrm{L(N)}$to fulfill the prime number theorem and consequently

$$\lim_{N\to\propto}\frac{L(N)}{N\ /logN}=1 \qquad (19)$$

In the table below up to integer N values of the prim counting function $\pi(\mathrm{N})$ approximation given by logarithmic integral $\mathrm{L}_i\,(\mathrm{N})$,$\mathrm{N/logN}$ the counting function $\mathrm{L(N)}$defined in equation

$$\mathrm{L(N)} = \mathrm{e} \propto \mathrm{(N)} \int_{\mathrm{Z}}^{\mathrm{N}} \mathrm{x}^{-\propto(\mathrm{N})}\,\mathrm{dx} \qquad (20)$$

And the ratio $L(\mathrm{N})/\pi(\mathrm{N})$.

Table 5.2.1 the function $\pi(\mathrm{N}\ )$ with different N given by logarithmic integral

N	$\pi(N)$	$L_i\,(N)$	$\mathrm{N/logN}$	$L(N)$	$\mathrm{L(N)}/\pi(N)$
10	25	30	22	29	0.85533
10	168	168	145	172	0.97595
10	1229	1246	1086	1228	1.00081
10	9592	9630	8686	9558	1.00352
10	78498	78628	72382	78280	1.00278
10	664579	6649189	620421	662958	1.00244
10	5761455	5762209	5428681	574998	1.00199
10	50847534	50849235	4825a4942	50767815	1.00157
10	455052511	45505561	434294432	45448488	1.00125
10	2220819602560918				1.00027

References

1. James Williamson (translator and commentator), *“The Elements of Euclid, With Dissertations”*, Clarendon Press, Oxford, 1782, page 63.
2. Selberg, Atle "*An elementary proof of Dirichlet's theorem about primes in an arithmetic progression*", Annals of Mathematics 50 (2): 297–304.

3. Nagell, T. 1951."*The Prime Number Theorem*" New York: Wiley, pp. 275-299,

4. Benjamin Fine, Gerhard Rosenberger "*Number Theory: An Introduction via the Distribution of Primes*" Birkhäuser Boston 2007.

5. Raimi, R,1969 "*The peculiar distribution of first digits*". Scientific American (December) pp. 109-119,.

6. Diaconis, P. 1977 "*The distribution of leading digits and uniform distribution mod 1*". Ann. Probab. 72–81.

7. B.Riemann "*Uber die Anzahl der Primzahlen unter einer gegbener Grosse Monatsber" ,*Kgl .Preuss ,Akad .Wiss .Berlin 1860, 671-680.

8. D.r. Stinsson ,"*Cryptography : Theory and Practice"* ,CRC Press ,Boca ,Fl ,2002.