Journal of Advances in Mathematics and Computer Science

36(7): 21-29, 2021; Article no.JAMCS.72335
ISSN: 2456-9968
(Past name: British Journal of Mathematics & Computer Science, Past ISSN: 2231-0851)

Possibility to Construct a Machine for Primality Testing of Numbers

Takaaki Musha[1,2*]

[1]Advanced Science-Technology Research Organization, Yokohama, Japan.
[2]Foundation of Physics Research Center (FoPRC), Cosenza, Italy.

Author's contribution

The sole author designed, analysed, interpreted and prepared the manuscript.

Article Information

DOI: 10.9734/JAMCS/2021/v36i730380
Editor(s):
(1) Mohd Zuki Salleh, Universiti Malaysia Pahang, Malaysia.
Reviewers:
(1) K Gurnadha Gupta, India.
(2) Amir Pishkoo, Iran.
Complete Peer review History: https://www.sdiarticle4.com/review-history/72335

Original Research Article

Received 15 June 2021
Accepted 21 August 2021
Published 23 August 2021

Abstract

Like the optical prism to break white light up into its constituent spectral colors, the machine to show a prime as a single spectrum is proposed. From the theoretical analysis, it can be shown that the machine to recognize the prime number as a single spectrum can be realized by using the correlation function of Riemann zeta function. Moreover, this method can be used for a factorization of the integer consisted of two primes.

Keywords: Prime; primality testing; Riemann zeta function; Platonic world factorization; savant syndrome.

1 Introduction

It would be interesting to know if number is a prime. There are some algorisms developed for primality testing of numbers. One of them is that a corollary of Fermat's little theorem which could be used to test for primality. it was shown in the Pocklington primality test. However, it requires a partial factorization of n-1 and the running time was quite slow in the worst case. The first deterministic primality test significantly faster than the conventional methods was the cyclotomy test; its runtime was proved to be $O((\log n)^{c \log\log\log n})$, where n is

**Corresponding author: Email: takaaki.mushya@gmail.com;*

the number to test for primality and c is a constant. Further improvements were made and the elliptic curve primality test was proved to run in $O((\log n)^6)$, if some conjectures on analytic number theory are true [1]. Similarly, under the generalized Riemann hypothesis, the deterministic Miller's test, which is the basis of the probabilistic Miller–Rabin test, was proved to run in $O((\log n)^4)$ [2]. The first provably deterministic polynomial time test for primality was invented by M.Agrawal, N. Kayal, and N.Saxena. The AKS primality test runs in $O((\log n)^{12})$ and which can be further reduced to $O((\log n)^6$, if the Sophie Germain conjecture is true [3]. Subsequently, Lenstra and Pomerance presented a version of the primality test which runs in time $O((\log n)^6$. Recently, Shor's algorithm has been proposed by Peter Shor, which is a quantum algorithm for integer factorization [4]. On a quantum computer, it has been proven that Shor's algorithm runs in polynomial time. But the polynomial time factoring algorithm of integers has not been found for ordinary computing systems. When the numbers are very large, no efficient, non-quantum integer factorization algorithm is known [5]. Hence the polynomial time factoring algorithm of integers is required to find for ordinary computing systems.

Instead of these primality testing methods and a factorization method of numbers, it is shown that the primality testing machine to recognize a prime as a single spectrum can be realized by using the Riemann zeta function. Furthermore, it can be shown that integer factorization can be conducted for the special case that the integer is consisted of two different primes. This result may explain some savant syndrome people exhibited an extraordinary ability to see the prime as an image after some unimaginable internal process of primality testing of numbers.

2 Theoretical Basis

Riemann zeta function is an analytic function defined by $\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$, which can also be given by

$$\zeta(s) = \prod_{p} \frac{1}{(1-p^{-s})} \tag{1}$$

which is the Euler product related to prime numbers.

We define the Fourier transform of $z_\sigma(t,\tau)$ shown as

$$Z_\sigma(t,\omega) = \lim_{T\to\infty} \int_{-T}^{+T} z_\sigma(t,\tau) e^{-i\omega\tau} d\tau\,, \tag{2}$$

where $z_\sigma(t,\tau)$ is a time-dependent autocorrelation function defined by

$z_\sigma(t,\tau) = \zeta(\sigma - i(t+\tau/2))\cdot\zeta^*(\sigma - i(t-\tau/2))$. In this formula, $\zeta^*(s)$ is a conjugate of $\zeta(s)$.

From the infinite sum of the Riemann zeta function given by $\zeta(\sigma - it) = \sum_{n=1}^{\infty} \frac{\exp(it\log n)}{n^\sigma}$, we have

$$Z_\sigma(t,\omega) = \lim_{T\to\infty} \int_{-T}^{+T} \sum_{k=1}^{\infty} \frac{1}{k^\sigma} \exp[i(t+\tau/2)\log k \times \sum_{l=1}^{\infty} \frac{1}{l^\sigma} \exp[i(t-\tau/2)\log l] e^{-i\omega t} dt$$

$$= \lim_{T\to\infty}\int_{-T}^{+T}\sum_{k,l}^{\infty}\frac{1}{(kl)^{\sigma}}\exp[i\log(k/l)t]\exp[i\log(kl)\tau/2]e^{-i\omega\tau}d\tau$$

For the integer n, we put $n = kl$, then we can write

$$Z_{\sigma}(t,\omega) = \lim_{T\to\infty}\sum_{k,l}^{\infty}\frac{1}{n^{\sigma}}\exp[i\log(k/l)t]\int_{-T}^{+T}\exp(i\tau\log n/2)e^{-i\omega\tau}d\tau,$$

where

$$\int_{-T}^{+T}\exp(i\tau\log n/2)e^{-i\omega\tau}d\tau = \frac{2\sin[(\omega-\frac{1}{2}\log n)]T}{(\omega-\frac{1}{2}\log n)}.$$

When we let $a(n,t) = \sum_{n=kl}\exp[i\log(k/l)t]$, Eq.(2) can be rewritten as

$$Z_{\sigma}(t,\omega) = \lim_{T\to\infty}\sum_{n=1}^{\infty}\frac{a(n,t)}{n^{\sigma}}\frac{2\sin[(\omega-\frac{1}{2}\log n)]T}{(\omega-\frac{1}{2}\log n)} = \sum_{n=1}^{\infty}\frac{a(n,t)}{n^{\sigma}}2\pi\delta(\omega-\tfrac{1}{2}\log n), \quad (3)$$

where $a(n,t)$ is a real valued function given by

$a(n,t) = \frac{1}{2}\sum_{n=kl}\{\exp[i\log(k/l)t] + \exp[i\log(l/k)t]\} = \sum_{n=kl}\cos[\log(k/l)t]$ and $\delta(\omega)$ is a Dirac's delta function.

At first, the author proposed two Lemmas, which were proved on the previous papers of author's shown as follows [6,7].

Lemma.1: $a(n,t)$ is a multiplicative on n.

From the definition of $a(n,t)$, we can obtain the following recurrence formula given by

$$a(p^{r},t) = a(p^{r-1},t)\cos(t\log p) + \cos(rt\log p) \ (r = 1,2,3\cdots), \quad (4)$$

From which, it can be proved that

$$a(p^{r},t) = \frac{\sin[(r+1)t\log p]}{\sin(t\log p)}, \quad (5)$$

From Eq.(3), we have $Z_{\sigma}(t,\frac{1}{2}\log n) = \frac{2\pi\delta(0)}{n^{\sigma}}a(n,t)$.

For the integer n given by $n = p^{a}q^{b}r^{c}\cdots$, we have

$$Z_\sigma(t,\tfrac{1}{2}\log n)=\frac{2\pi\delta(0)}{n^\sigma}\frac{\sin[(a+1)t\log p]}{\sin(t\log p)}\times\frac{\sin[(b+1)t\log q]}{\sin(t\log q)}\times\frac{\sin[(c+1)t\log r]}{\sin(t\log r)}\cdots$$

from Lemma.1 and Eq.(5).

From the Fourier transform of $Z_\sigma(t,\frac{1}{2}\log n)$ given by $F_n(\omega)=\int_{-\infty}^{+\infty}Z_\sigma(t,\frac{1}{2}\log n)e^{-i\omega t}dt$, we can obtain the following Lemma [7].

Lemma.2; If $n=p_1p_2p_3\cdots p_k$, where $p_1,p_2,p_{3,}\cdots p_k$ are different primes, $F_n(\omega)$ is consisted of 2^{k-1} discrete spectrums.

Then we obtain following Theorems.

Theorem. I; If and only $F_n(\omega)$ is consisted of a single spectra for $\omega\geq 0$, then n is a prime.

Proof; The Fourier transform of $\cos(t\log p)$ can be given by $\pi[\delta(\omega-\log p)+\delta(\omega+\log p)]$, and thus it is clear from Lemma.2. (QED)

Theorem. II; If and only $F_n(\omega)$ is consisted of two spectrum for $\omega\geq 0$, then n has the form of $n=p\cdot q$ ($p\neq q$), otherwise $n=p^2$ or $n=p^3$.

Proof; From Theorem I, there is only a case for the integer $n=p_1p_2\cdots p_k$, when $F_n(\omega)$ is consisted of two spectrum, that is $n=p\cdot q$ ($p\neq q$).

From Eq.(4), we have following equations for $a(p^r,t)$;

$r=1,\ a(p,t)=2\cos(t\log p)$
$r=2,\ a(p^2,t)=1+2\cos(2t\log p)$
$r=3,\ a(p^3,t)=2\cos(t\log p)+2\cos(3t\log p)$
$r=4,\ a(p^4,t)=1+2\cos(2t\log p)+2\cos(4t\log p)$
$r=5,\ a(p^5,t)=2\cos(t\log p)+2\cos(3t\log p)+2\cos(5t\log p)$
$r=6,\ a(p^6,t)=1+2\cos(2t\log p)+2\cos(4t\log p)+2\cos(6t\log p)$
$r=7,\ a(p^7,t)=2\cos(t\log p)+2\cos(3t\log p)+2\cos(5t\log p)+2\cos(7t\log p)$

Including the spectrum at $\omega=0$, there are cases for $r=2$ and $r=3$ when $a(n,t)$ has two spectrums.

(QED)

Theorem. III: If $F_n(\omega)$ is consisted of two spectrums at frequencies ω_1 and ω_2, and we let $n=p\cdot q$, we can obtain factors of an integer n given by

$$p=\exp\left(\frac{\omega_2-\omega_1}{2}\right)\text{ and }q=\exp\left(\frac{\omega_1+\omega_2}{2}\right).$$

Proof; If $n=pq$, then we obtain

$$Z_\sigma(t,\tfrac{1}{2}\log n)=\frac{4\pi\delta(0)}{n^\sigma}\cos(t\log p)\times\cos(t\log q)$$

$$=\frac{2\pi\delta(0)}{n^\sigma}\{\cos[(\log q-\log p)t]+\cos[(\log q+\log p)t]\}.$$

When we let $\omega_1=\log q-\log p$, and

$\omega_2=\log q+\log p$, we have

$$p=\exp\left(\frac{\omega_2-\omega_1}{2}\right),\ q=\exp\left(\frac{\omega_1+\omega_2}{2}\right)$$

(QED)

3 How to Construct the Machine for Primality Testing

From Theorems I, II and III, we can make a primality testing and a factorization of the integer n consisted of two primes from the Fourier spectrum $F_n(\omega)\ \ (\omega\geq 0)$ by following procedure;

At first, compute the Fourier transform $Z_\sigma(t,\omega)=\int_{-\infty}^{+\infty}z_\omega(t,\tau)e^{-i\omega\tau}d\tau$, where $z_\sigma(t,\tau)=\zeta(\sigma-i(t+\tau/2))\cdot\zeta^*(\sigma-i(t-\tau/2)$, from which we can obtain the Fourier spectrum given by $F_n(\omega)=\int_{-\infty}^{+\infty}Z_\sigma(t,\tfrac{1}{2}\log n)e^{-i\omega t}dt$. Then we can make a primality testing from the process shown as follows;

① Generating the zeta function by $\zeta(s)=\frac{1}{d_0(1-2^{1-s})}\sum_{k=1}^{n}\frac{(-1)^{k-1}d_k}{k^s}+\gamma_n(s)$

where

$$d_k=n\sum_{j=k}^{n}\frac{(n+j-1)!4^j}{(n-j)!(2j)!}$$

and

$$|\gamma_n(s)|\leq\frac{3}{(3+\sqrt{8})^n}\frac{(1+2^{|t|})e^{|t|\pi/2}}{|1-2^{1-s}|}\ \text{with}\ n\approx 1.3d+0.9|t|.$$

From which, we can compute $\zeta(\sigma+it)$ with d decimal digits of accuracy [8].

② Compute the correlation function by $z_\sigma(t,\tau)=\zeta(\sigma-i(t+\tau/2))\cdot\zeta^*(\sigma-i(t-\tau/2))$

③ Conduct Fourier transform given by $Z_\sigma(t,\omega)=\int_{-\infty}^{+\infty}z_\sigma(t,\tau)e^{-i\omega\tau}d\tau$

④ Conduct Fourier transform given by $F_n(\omega) = \int_{-\infty}^{+\infty} Z_\sigma(t, \frac{1}{2}\log n) e^{-i\omega t} dt$

To conduct calculations to obtain the values of $F_n(\omega)$ by using discrete Fourier transform, we can select the value for frequency resolution as $\Delta f = 1/4\pi n$ from $\Delta\omega = \left|\frac{1}{2}\log n - \frac{1}{2}\log(n \pm 1)\right| \approx 1/2n$, for large numbers. Then we select the maximum frequency of DFT analysis to be $f_{\max} = 4[\log n / 4\pi]$ (where [ ] is a Gauss's symbol), which makes $\omega = \log n$ to be at the center of frequency range.

The element number N for DFT calculation satisfies $f_{\max} = N \cdot \Delta f / 2$, then we have $N = [8n \log n] + 1$.

Fig. 1 is the machine for primality testing of a natural number, and ①,②,③ and ④ in Fig. 1 correspond to the number of above calculations.

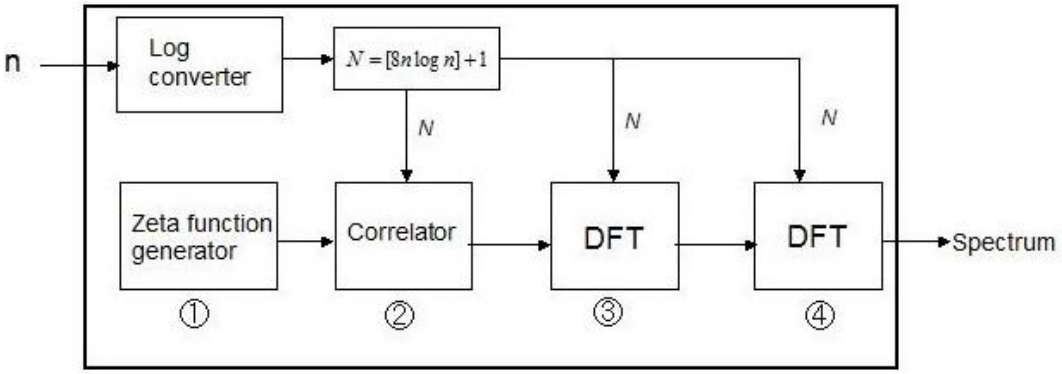

Fig. 1. Diagram of the machine for primality testing

As the number ② can be written in a discrete form as

$$z(m,l) = \zeta(\sigma - i(m\Delta t + l\Delta\tau/2)) \cdot \zeta^*(\sigma - i(m\Delta t - l\Delta\tau/2)).$$

From the relation of $\Delta f \cdot \Delta t = 1/N$, we obtain

$$z(m,l) = \zeta\left(\sigma - i\left(\frac{4\pi n}{N}m + \frac{2\pi n}{N}l\right)\right) \cdot \zeta^*\left(\sigma - i\left(\frac{4\pi n}{N}m - \frac{2\pi n}{N}l\right)\right).$$

As the total time $T_0 = N \cdot \Delta t = 4\pi n$, then the number ③ in a discrete form can be given by

$$Z(m,k) = \frac{4\pi n}{N}\sum_{l=0}^{N-1} z(m,l)\exp[-i2\pi(k\Delta f)\cdot(l\Delta\tau)] \ .$$

At the frequency of $\omega = \frac{1}{2}\log n$, we have $k\Delta f \cdot l\Delta\tau = \frac{\log n}{4\pi} \times \frac{\pi}{2\log n} l = \frac{l}{8}$,

then we have $y(m) = \frac{4\pi n}{N}\sum_{l=0}^{N-1} z(m,l)\exp\left(-i\frac{\pi}{4}l\right)$, which corresponds to $Z_\sigma(t, \frac{1}{2}\log n)$.

From which, we have the discrete form of the number ④ given by

$$Y(k)=\frac{4\pi n}{N}\sum_{m=0}^{N-1}y(m)\exp\left(-i2\pi\frac{km}{N}\right)$$, which shows the spectrum of $F_n(\omega)$.

Thus discrete forms of equations ②,③ and ④ are shown as follows [9];

② When we let $N=[8n\log n]+1$, conduct calculation

$$z(m,l)=\zeta\left(\sigma-i\left(\frac{4\pi n}{N}m+\frac{2\pi n}{N}l\right)\right)\cdot\zeta^{*}\left(\sigma-i\left(\frac{4\pi n}{N}-\frac{2\pi n}{N}l\right)\right)$$

③ Conduct DFT, $m=0\sim N-1$;

$$y(m)=\frac{4\pi n}{N}\sum_{l=0}^{N-1}z(m,l)\exp\left(-i\frac{\pi}{4}l\right)$$

④ Conduct DFT, $k=0\sim N-1$;

$$Y(k)=\frac{4\pi n}{N}\sum_{m=0}^{N-1}y(m)\exp\left(-2i\pi\frac{km}{N}\right)$$

4 Results and Discussion

To confirm the validity of discrete computational algorism given in this paper, the author tries to compute some examples shown as follows;

In the calculation, the author selected $\sigma=1.1$ to compute $F_n(\omega)$ to minimize the noise generated by DFT calculations. By using the above discrete calculation, we have calculation results for the prime (n=17) and the number consisted of two primes (n=21) as shown in Fig. 2 [10]. From which, it can be seen that we can recognize the prime as a single spectrum. We can also recognize two spectrums for the number consisted of two primes and thus we can make a factorization of the number consisted of two primes.

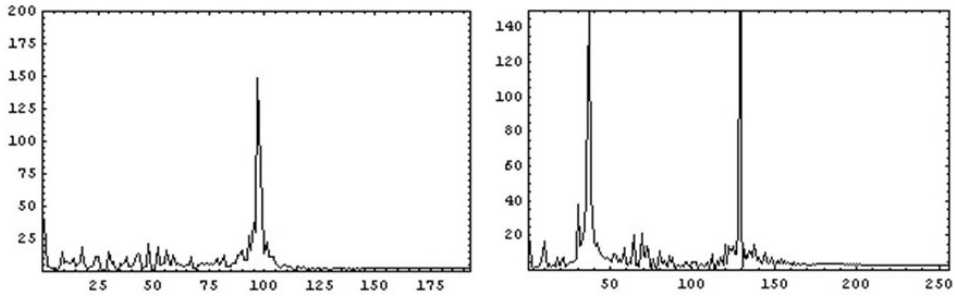

Fig. 2. Spectrum obtained for a prime (Left) and spectrums for the number consisted of two primes (Right)

This result may explain some savant syndrome people exhibited an extraordinary ability to see the prime as an image after some unimaginable internal process. Olver Sacks mentioned in his book, "The Man Who Mistook His Wife for a Hat" [11], on the twins, John and Michael, who were idiot savants, who exhibited a mysterious

human ability on primes using unconscious algorithm. They seemed to have a peculiar passion and grasp of numbers even for they could not calculate, and lack even the most rudimentary powers of arithmetic. In front of Dr.Sacks, they exhibited an extraordinary ability to see the eight-digit number as a prime after some unimaginable internal process of testing. After that time, the twins were able to swap twenty-figure primes, which are difficult even for computers to uses Eratosthenes's sieve or any other algorithm.

There is no simple method of calculating primes. He supposed that they visualize prime patters instead of calculation, but the riddle how they visualized the primes and used them for communication to each other leaves unanswered.

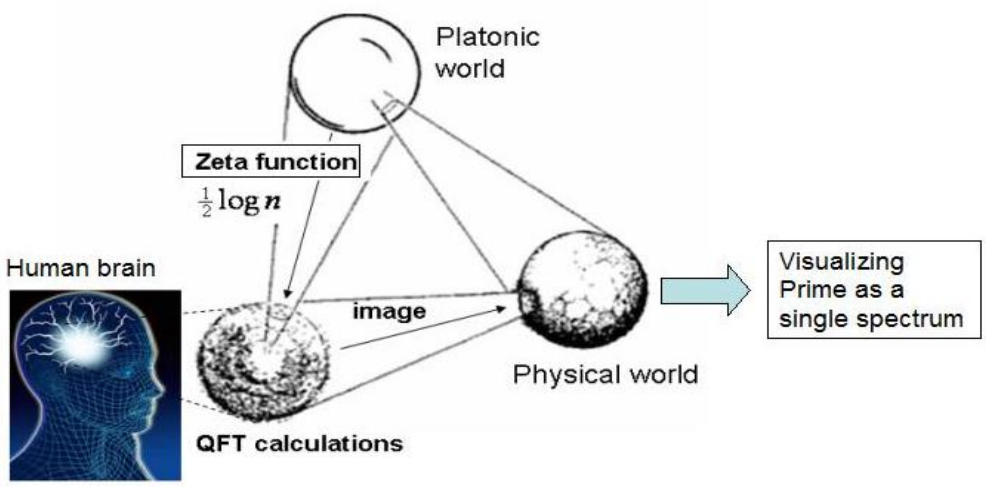

Fig. 3. Penrose three world and the mechanism of the human brain to recognize prime numbers as an image (QFT: Quantum Fourier Transform)

In Penrose's metaphysical framework, there are three forms of existence or "worlds": the physical, the mental, and the Platonic mathematical entities as shown in Fig.3.

He claimed that mathematical entities are real in the mathematical Platonic world [12]. If the human brain is a quantum computer as claimed by Penrose, it can be seen that the primality testing and integer factorization of the integer n consisted of two primes can be conducted efficiently by using the information on zeta function as shown in the previous section. Supposing that the human brain is a quantum computer as claimed by Penrose [12] and it can create the correlation function by using the Riemann zeta function from the Platonic world as shown in Fig.3, some savant syndrome people can visualize primes as an image after an internal process of calculation. Then the riddle of the twins, John and Michael, may be solved.

5 Conclusion

From the spectrum obtained by the Fourier transform of a correlation function generated from the Riemann zeta function, we can see the primality of an integer n if and only the $F_n(\omega)$ has a single spectrum for $\omega \geq 0$. Furthermore, it can be shown that factorization of numbers can be conducted within a polynomial time for the special case that the integer is consisted of two different primes and hence we can conclude that factorization for the integer consisted of two different primes is in the P class. Hence this method can be applied to break the RSA cryptosystem.

Competing Interests

Author has declared that no competing interests exist.

References

1. Yan SY. Number Theory for Computing: Springer-Verlag, New York; 1998.
2. Miller GL. Riemann's hypothesis and tests for primality, Journal of Computer and System Sciences. 1976;13(3); 300-317.
3. Agrawal M, Kayal N, Saxena N. Prime is in P, Annals of Mathematics. 2004;160(2):781-793.
4. Shor PW. Polynomial-time algorithm for prime factorization and discrete logarithm on quantum computer, SIAM.J. Comput. 1997;26(5):1484-1509.
5. Nielsen MA, Chuang IL. Quantum computation and quantum information, Cambridge University Press, Cambridge; 2000.
6. Musha T. A study on the riemann hypothesis by the wigner distribution analysis, JP Journal of Algebra, Number Theory and Applications. 2012;24:137-147.
7. Musha T. Primarity Testing and Integer Factorization by using Fourier Transform of a Correlation Function generated from the Riemann Zeta Function, Theory and Applications of Mathematics & Computer Science. 2014;4(2):1-7.
8. Gourdon X, Sebah P. Numerical evaluation of the Riemann Zeta-Function; 2003. Available:http.//numbers.Computation.free.fr/Constants/Miscellaneous/zetaevaluations.pdf
9. Musha T. Primary testing and factorization by using Fourier spectrum of Riemann zeta function, Theory and Applications of Mathematics & Computer Science. 2015;5(2):213-220.
10. Musha T. Mathematical Zeta Prism for Primality Testing, International Journal of Pure Mathematics. 2019;6:8-13.
11. Sacks O. The Man who mistook his wife for a Hat: Picador; 1986.
12. Penrose R. The Large, the Small and the Human Mind: Cambridge University Press; 1997.

Peer-review history:
The peer review history for this paper can be accessed here (Please copy paste the total link in your browser address bar)
https://www.sdiarticle4.com/review-history/72335