Mathematical Zeta Prism for Primarity Testing

Takaaki Musha

Abstract- Like the optical prism, the mathematical prism for the use of primality testing of numbers is proposed. From the theoretical analysis, it can be shown that the mathematical prism to recognize the prime numbers as a single spectra can be realized by using Riemann zeta function. Moreover, this method can be used for a factorization of the integer n consisted of two primes.

Key word- prime, primality testing, Riemann zeta function, Platonic world

I. INTRODUCTION

In optics, a prism is a transparent optical element with flat, polished surfaces that refract light. Light changes speed as it moves from one medium to another. This speed change causes the light to be refracted and to enter the new medium at a different angle . The degree of bending of the light's path depends on the angle that the incident beam of light makes with the surface, and on the ratio between the refractive indices of the two media. The refractive index of many materials varies with the wavelength or color of the light used, a phenomenon known as dispersion.

Takaaki Musha is with the Advanced Science-Technology Research Organization, Yokohama, Japan.

(e-mail: takaaki.mushya@gmail.com)

This causes light of different colors to be refracted differently and to leave the prism at different angles, creating an effect similar to a rainbow. This can be used to separate a beam of white light into its constituent spectrum of colors.

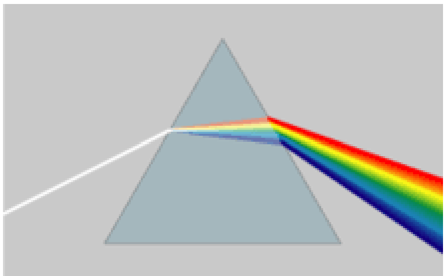

Figure.1 Prism which separates light into monotonic colors

Similar to a optical prism, the author consider a mathematical prism which can separate numbers into primes, those consist natural numbers. For this purpose, the Riemann zeta function is utilized. A primality test is a computer algorithm for determining whether an input number is prime. Some primality tests prove that a number is prime or not, while others like Miller–Rabin prove that a number is composite. Therefore, the latter might more accurately be called compositeness tests instead of primality tests.

The mathematical prism method can state that a number is composite or not like the Miller-Rabin test and make the factorization of the number consisted of two primes .

II. FREQUENCY SPETRUM OF A CORRELATIONN FUNCTION GENERAATED FROM THE- RIEMANN ZETA FUNCTION

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

$$\zeta(s)=\frac{1}{\Gamma(s)}\int_0^{\infty}\frac{x^{s-1}}{e^x-1}dx \ (\mathrm{Re}[s]>1), \quad (1)$$

where $\Gamma(s)$ is a Gamma function.

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

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

where $z_\sigma(t,\tau)$ is a time-dependent autocorrelation function [2] 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

$$\mathrm{Z}_\sigma(t,\omega)=\lim_{T\to\infty}\int_{-T}^{+T}\sum_{k=1}^{\infty}\frac{1}{k^\sigma}\exp[i(t+\tau/2)\log k$$

$$\times\sum_{l=1}^{\infty}\frac{1}{l^\sigma}\exp[i(t-\tau/2)\log l]e^{-i\omega t}dt$$

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

For the integer n, 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

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

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.

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

Proof: As we can write

$$a(n,t)=\sum_{n=kl}\exp[i\log(k/l)t],$$

the multiplicative property of which can be shown from

$$a(n,t)=\sum_{k|n}\exp\left(it\log(k^2/n)\right)=\frac{1}{n^{it}}\sum_{k|n}k^{2it}$$

If $f(n)$ is multiplicative, then $F(n)=\sum_{d|n}f(d)$ is multiplicative. From which, we have $a(mn,t)=a(m,t)a(n,t)$ for the case when. satisfying $(m,n)=1$, because k^{2it} is multiplicative. (QED)

From the definition of $a(n,t)$, we can obtain the following recurrence formula given by [3]

$$a(p^r,t)=a(p^{r-1},t)\cos(t\log p)+\cos(rt\log p)$$

($r = 1,2,3\cdots$), (4)

From which, it can be proved that

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

From Eq.(3), we have

$$Z_\sigma(t, \tfrac{1}{2}\log n) = \frac{2\pi\delta(0)}{n^\sigma} a(n,t).$$

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

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

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.

Lemma.2; If $n = p_1 p_2 p_3 \cdots p_k$, where $p_1, p_2, p_{3,} \cdots p_k$ are different primes, $F_n(\omega)$ is consisted of 2^{k-1} discrete spectrum.

Proof: From Eq.(4), we have

$$a(n,t) = 2\cos(t\log p_1)\cdot 2\cos(t\log p_2)$$
$$\times 2\cos(t\log p_3)\cdots 2\cos(t\log p_k)$$

By the trigonometrical formula,

$\cos\alpha \cdot \cos\beta = \frac{1}{2}\{\cos(\alpha-\beta) + \cos(\alpha+\beta)\}$, we have

$$a(n,t)$$
$$= 2\times\frac{1}{2}\{\cos[(\log p_1 - \log\ p_2)t] + \cos[(\log p_1 + \log p_2)t]\}$$
$$\times 2\cos(\log p_3 \cdot t)\cdots 2\cos(\log p_k \cdot t)$$
$$= \{\cos[(\log p_1 - \log p_2)t]\cos(\log p_3 \cdot t)$$
$$+ \cos[(\log p_1 + \log p_2)t]\cos(\log p_3 \cdot t)\}$$
$$\cdots 2\cos(\log p_k \cdot t)$$
$$= \{\cos[(\log p_1 - \log p_2 - \log p_3)t] + \cos[(\log p_1 - \log p_2 + \log p_3)t]$$
$$+ \cos[(\log p_1 + \log p_2 - \log p_3)t]$$
$$+ \cos[(\log p_1 - \log p_2 + \log p_3)t]\}\cos(\log p_4 \cdot t)\cdots 2\cos(\log p_k \cdot t)$$

By the repetition of above computation, we have

$$a(n,t) = \sum_{i=1}^{2^k} [\cos(\lambda_{i1}\log p_1) + \cos(\lambda_{i2}\log p_2) + \cdots \cos(\lambda_{ik}\log p_k)]$$

where λ_{ik} equals to -1 or +1.

As $\log p_1, \log p_2, \log p_3, \cdots \log p_k$ are linearly independent over **Z** [4] , thus $F_n(\omega)$ is consisted of 2^{k-1} different spectrum. (QED)

Then we obtain following Theorems.

Theorem.I; If and only $F_n(\omega)$ is consisted of a single spectra for $\omega \ge 0$, 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 $\omega \ge 0$, then n has the form of $n = p\cdot q$ ($p \ne q$), otherwise $n = p^2$ or $n = p^3$.

Proof; From Theorem I, there is only a case for the integer $n = p_1 p_2 \cdots p_k$, when $F_n(\omega)$ is consisted of two spectrum, that is $n = p\cdot q$ ($p \ne q$).

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

$r = 1$, $a(p,t) = 2\cos(t\log p)$

$r = 2$, $a(p^2,t) = 1 + 2\cos(2t\log p)$

$r = 3$, $a(p^3,t) = 2\cos(t\log p) + 2\cos(3t\log p)$

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

$r = 5$, $a(p^5,t) = 2\cos(t\log p) + 2\cos(3t\log p)$
$\quad + 2\cos(5\log p)$

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

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

$$+2\cos(5t\log p)+2\cos(7t\log p)$$
$$\vdots$$

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

Theorem. III: If $F_n(\omega)$ is consisted of two spectrums at frequencies ω_1 and ω_2 and $n = p \cdot q$, 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)

III. RIMARITY TESTING AND FACTIRIZATION BY THE MATHEMATICAL ZETA PRIISM

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 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 as shown Fig.2.

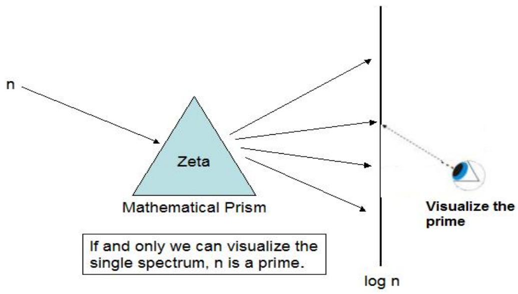

Figure.2 Mathematical prism by using the zeta function to conduct a primality test for the integer n

From the process as shown in Fig.3, we can recognize the prime as a single spectra from the frequency analysis result [5]. If there are two spectrum observed from the calculation result, n has the form of $n = p \cdot q$ ($p \neq q$), otherwise $n = p^2$ or $n = p^3$.

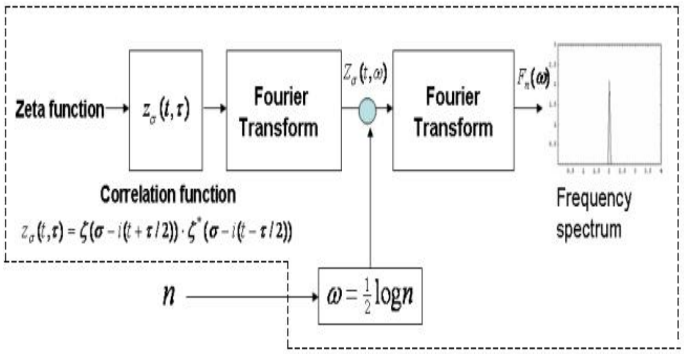

Figure.3 Structure of the mathematical zeta prism

In this case, we can obtain factors of an integer n from Theorem.III.

It is known that Fourier transform can be conducted by the quantum computer, the schematic diagram for the quantum Fourier transform is shown in Fig.4 [6].

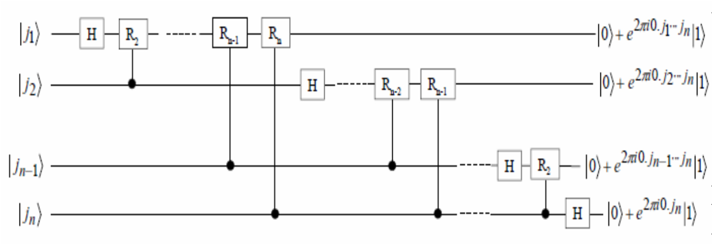

Figure. 4 Schematic diagram for the quantum Fourier transform

In this figure, H is a Hadamard gate and R_k is a unitary transformation given by $R_k = \begin{bmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^k} \end{bmatrix}$.

From this result, we can visualize the prime as a single frequency spectrum (that is monochromatic light).

Calculation results by using FFT algorism are shown as follows [5]:

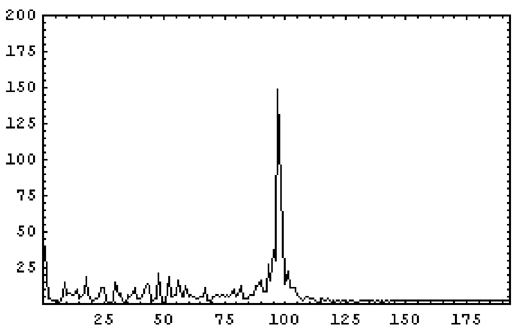

Figure.5 Calculation result for the prime

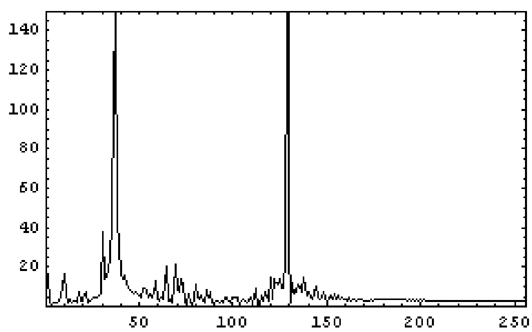

Figure.6 Calculation result for the number consisted of two primes

IV. POSSIBILITY OF THE BRAIN WHICH CAN FUNCTIONN AS A MATHEMATICAL ZETA PRISM

Olver Sacks mentioned in his book, "The Man Who Mistook His Wife for a Hat"[7], 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.

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.7.

He claimed that mathematical entities are real in the mathematical Platonic world [8].

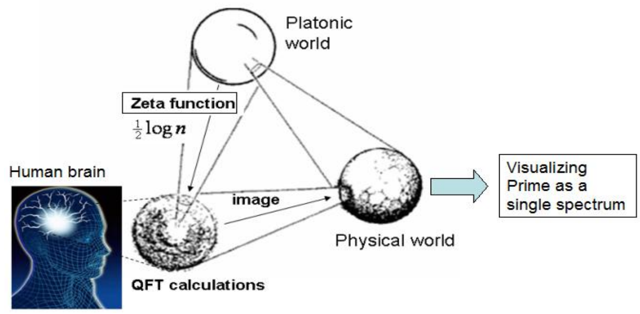

Figure.7 Penrose three world and the mechanism of the human brain to recognize prime numbers

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.

Supposing that the human brain is a quantum computer as claimed by Penrose [8] and it can create the mathematical zeta prism by using the Riemann zeta function from the Platonic world as shown in Fig.7, we can visualize the prime. Then the riddle of the twins, John and Michael, can be solved.

V. CONCLUSION

From the spectrum obtained by the Fourier transform of a correlation function generated from the Riemann zeta function given by

$F_n(\omega) = \int_{-\infty}^{+\infty} Z_\sigma(t, \frac{1}{2}\log n) e^{-i\omega t} dt$, we can see that the mathematical prism to recognize the prime numbers as a single spectra.

This method can be applied for the computer algorithm to prove if the number is a prime or not. Furthermore, if the mathematical Platonic world does exist as claimed by Penrose, the human brain has a possibility to recognize prime numbers as a visualized pattern reported by Oliver Sacks.

REFEENCS

[1] G.H. Hardy, M. Riesz, The General Theory of Dirichlet’s Series, Dover Publications, Inc., Mineola, N.Y. 2005.

[2] N.Yen, Time and frequency representation of acoustic signals by means of the Wigner distribution function: Implementation and interpretation, J.Acoust. Soc.Am.81(6), 1987, pp.1841-1850.

[3] T.Musha, A Study on the Riemann Hypothesis by The Wigner Distribution Analysis, JP Journal of Algebra, Number Theory and Applications, Vol.24, No.2, 2012, pp.137-147.

[4] M.Kac, Statistical Independence in Probability Analysis and Number Theory, The Mathematical Association of America, 1959.

[5] T.Musha, Primality Testing and Factorization by using Fourier Spectrum of the Riemann Zeta Function, Theory and Applications of Mathematics & Computer Science, 5(2), 2015, pp.213-226.

[6] M.A.Nielsen and I.L.Chuang, Quantum Computation and Quantum Information, Cambridge University Press, Cambridge, 2000.

[7] O.Sacks, The Man who mistook his wife for a Hat, Picador, 1986.

[8] R.Penrose, The Large, the Small and the Human Mind, Cambridge University Press, 1997.