Theory and Applications of
Mathematics & Computer Science

(ISSN 2067-2764, EISSN 2247-6202)
http://www.uav.ro/applications/se/journal/index.php/tamcs

Theory and Applications of Mathematics & Computer Science 4 (2) (2014) 185–191

# Primality Testing and Integer Factorization by using Fourier Transform of a Correlation Function Generated from the Riemann Zeta Function

Takaaki Musha[a,*]

[a]*Advanced Science-Technology Research Organization 3-11-7-601, Namiki, Kanazawa-ku, Yokohama 236-0005 Japan.*

## Abstract

In this article, the author tries to make primarity testing and factorization of integers by using Fourier transform of a correlation function generated from the Riemann zeta function.

*Keywords:* Primarity testing, factorization, Fourier transform, Riemann zeta function.
*2010 MSC:* 11A51, 11M06, 11Y05, 11Y11, 42A38.

## 1. Introduction

In number theory, integer factorization or prime factorization is the decomposition of a composite number into smaller non-trivial divisors, which when multiplied together equal the original integer. When the numbers are very large, no efficient, non-quantum integer factorization algorithm is known; an effort by several researchers concluded in 2009, factoring a 232-digit number (RSA-768), utilizing hundreds of machines over a span of 2 years. The presumed difficulty of this problem is at the heart of widely used algorithms in cryptography such as RSA (Rivest *et al.*, 1978). Many areas of mathematics and computer science have been brought to bear on the problem, including elliptic curves, algebraic number theory, and quantum computing.

In this article, the author tries to make primarity testing and factorization of integers by using Fourier transform of a correlation function generated from the Riemann zeta function.

[*] Corresponding author
*Email address:* takaaki.mushya@gmail.com (Takaaki Musha )

## 2. Frequency Spectrum of a Correlation Function generated 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 (Hardy & Riesz, 2005).

$$\zeta(s) = \frac{1}{\Gamma(s)} \int_0^{\infty} \frac{x^{s-1}}{e^x - 1} dx \quad (\mathrm{Re}[\, s\,] > 1)\,, \tag{2.1}$$

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

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

$$Z_\sigma(t, \omega) = \lim_{T\to\infty} \int_{-T}^{+T} z_\sigma(t, \tau) e^{-i\omega\tau} d\tau\,, \tag{2.2}$$

where $z_\sigma(t, \tau)$ is a time-dependent autocorrelation function (Yen, 1987) 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

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

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

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

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

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

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

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

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

$$a(n,t) = \frac{1}{2}\sum_{n=kl}\left\{\exp\left[i\log(k/l)\,t\right] + \exp\left[i\log(l/k)\,t\right]\right\} = \sum_{n=kl}\cos\left[\,\log(k/l)\,t\,\right]$$

and $\delta(\omega)$ is a Dirac's delta function.

**Lemma 2.1.** *$a(n,t)$ 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

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

where the subscript $k|n$ indicates integers $k$ which divide $n$ .

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. □

From the definition of $a(n,t)$ , we can obtain the following recurrence formula given by (Musha, 2012).

$$a(p^r,t) = a(p^{r-1},t)\cos(t\log p) + \cos(rt\log p) \quad (r = 1,2,3,\cdots). \tag{2.3}$$

From which, it can be proved that $a(p^r,t) = \dfrac{\sin[(r+1)t\log p]}{\sin(t\log p)}$. (2.4)

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

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

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

from Lemma.1 and Eq.(5).

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

**Lemma 2.2.** *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 spectrum.*

*Proof.* From Eq. (4), we have

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

By the trigonometrical formula shown as $\cos\alpha \cdot \cos\beta = \frac{1}{2}\{\cos(\alpha-\beta)+\cos(\alpha+\beta)\}$ , we have

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

$$= 2^2 \left\{\cos[t(\log p_1 - \log p_2)]\cos(t\log p_3) \quad + \cos[t(\log p_1 + \log p_2)]\cos(t\log p_3)\right\}\cdots 2\cos(t\log p_k)$$

$$= 2^2 \times \frac{1}{2}\left\{\cos[t(\log p_1 - \log p_2 - \log p_3)] \;+ \cos[t(\log p_1 - \log p_2 + \log p_3)]\right.$$

$$\left. + \cos[t(\log p_1 + \log p_2 - \log p_3)] + \cos[t(\log p_1 + \log p_2 + \log p_3)]\right\} 2\cos(t\log p_4)\cdots 2\cos(t\log p_k)$$

By repeating the above computations, we have

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

where $\lambda_{i1} = +1$ and $\lambda_{ij} = +1$ or $-1$ for $j > 1$.

As $\log p_1$, $\log p_2$, $\log p_3$, $\cdots$ , $\log p_k$ are linearly independent over **Z** (Kac, 1959), thus $F_n(\omega)$ is consisted of $2^{k-1}$ different spectrum. □

Then we obtain following Theorems.

**Theorem 2.1.** *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 2.2. □

**Theorem 2.2.** *If and only $F_n(\omega)$ is consisted of two spectrum for $\omega \geq 0$ , then n has either form of $n = p \cdot q\ (p \neq q)$ , $n = p^2$ 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 $n = p \cdot q \quad (p \neq q)$ .

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

$$\begin{aligned}
r = 1,\ & a(p,t) \;\, = 2\cos(t\log p)\\
r = 2,\ & a(p^2,t) = 1 + 2\cos(2t\log p)\\
r = 3,\ & a(p^3,t) = 2\cos(t\log p) + 2\cos(3t\log p)\\
r = 4,\ & a(p^4,t) = 1 + 2\cos(2t\log p) + 2\cos(4t\log p)\\
r = 5,\ & a(p^5,t) = 2\cos(t\log p) + 2\cos(3t\log p) + 2\cos(5t\log p)\\
r = 6,\ & a(p^6,t) = 1 + 2\cos(2t\log p) + 2\cos(4t\log p) + 2\cos(6t\log p)\\
r = 7,\ & a(p^7,t) = 2\cos(t\log p) + 2\cos(3t\log p) + 2\cos(5t\log p) + 2\cos(7t\log p)\\
& \vdots
\end{aligned}$$

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

**Theorem 2.3.** *If $F_n(\omega)$ is consisted of two spectrums at frequencies $\omega_1$ and $\omega_2$ and $n = p \cdot q$ , we can obtain factors of an integer n given by $p = \exp\left(\frac{\omega_2 - \omega_1}{2}\right)$ and $q = \exp\left(\frac{\omega_1 + \omega_2}{2}\right)$.*

*Proof.* If $n = p \cdot q$ , then we obtain $Z_\sigma\left(t, \frac{1}{2}\log n\right) = \frac{4\pi\delta(0)}{n^\sigma} \times \cos(t\log p) \cdot \cos(t\log q) = \frac{2\pi\delta(0)}{n^\sigma}\left\{\cos[(\log q - \log p)t] + \cos[(\log q + \log p)t]\right\}$.

When we let $\omega_1 = \log q - \log p$ , $\omega_2 = \log q + \log p$ , we have $p = \exp\left(\frac{\omega_2 - \omega_1}{2}\right)$ , $q = \exp\left(\frac{\omega_1 + \omega_2}{2}\right)$. □

## 3. Primarity Testing and Factorization from Fourier spectrum

From Theorems 2.1, 2.2 and 2.3, we can make primality testing and factorization of the integer $n$ consisted of two primes from the Fourier spectrum $F_n(\omega)$ $(\omega \geq 0)$ by following procedures;

At first, compute the Fourier transform $Z_\sigma(t,\omega) = \int_{-\infty}^{+\infty} z_\sigma(t,\tau)e^{-i\omega\tau}d\tau$, 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 $F_n(\omega) = \int_{-\infty}^{+\infty} Z_\sigma\left(t, \frac{1}{2}\log n\right)e^{-i\omega t}dt$. Then we can make primality testing and integer factorization of an integer $n$, the process of which is shown in Figure 1.

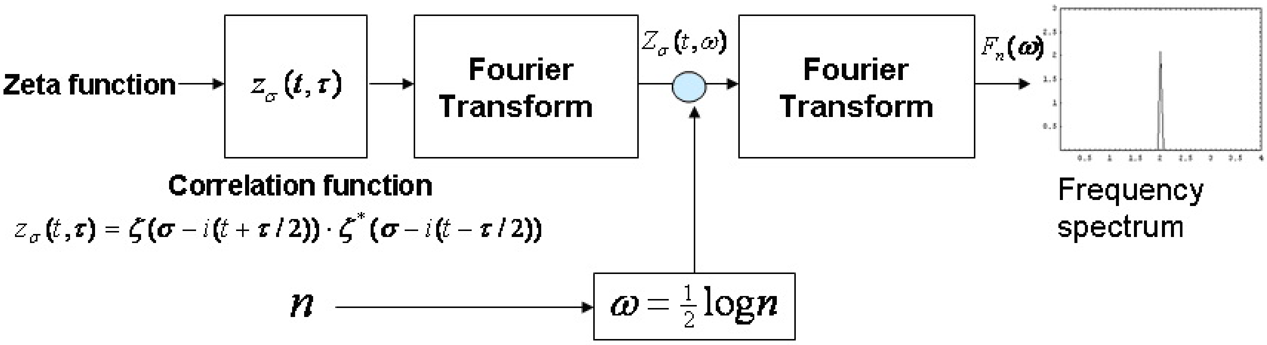

**Figure 1.** Process to conduct primality testing for the integer $n$.

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

In this case, we can obtain factors of an integer $n$ from Theorem 2.3.

As the Fourier transform $Z_\sigma(t,\omega) = \int_{-\infty}^{+\infty} z_\sigma(t,\tau)e^{-i\omega\tau}d\tau$ can be computed by using discrete FFT (fast Fourier transform) algorithm for the calculation of Wigner distribution function (Boashash & Black, 1987), (Dellomo & Jacyna, 1991) because $Z_\sigma(t,\omega)$ can be regarded as a Wigner distribution of the Riemann's zeta function, we can obtain the Fourier spectrum of $F_n(\omega)$ by conducting FFT calculations.

By using this method, we can propose some possible applications which use the theory presented in this paper.

- Primary testing of large numbers such as Mersenne numbers $2^m - 1$ can be conducted by using the algorithm shown in Figure 1 from the approximation, $\omega = \frac{1}{2}\log(2^m - 1) = \frac{m}{2}\log 2 - 1/2^{m+1} - 1/2^{2m+2} - \cdots$ .

- Factorization of an integer $n$ consisted of two primes can be conducted by using this method. By using FFT algorithm, there is a possibility to complete the computation within a polynomial time, whereas there is no known efficient algorithm that runs in polynomial time (Ribenboim, 1991).

- Breaking the public-key crypto system, which is considered to be hard by using the conventional computer systems, because the RSA crypto-system depends on the factorization of an integer composed of two large primes.

It is also known that Fourier transform can be conducted by the quantum computer, the schematic diagram for the quantum Fourier transform is shown in Figure 2 (Nielsen & Chuang, 2000).

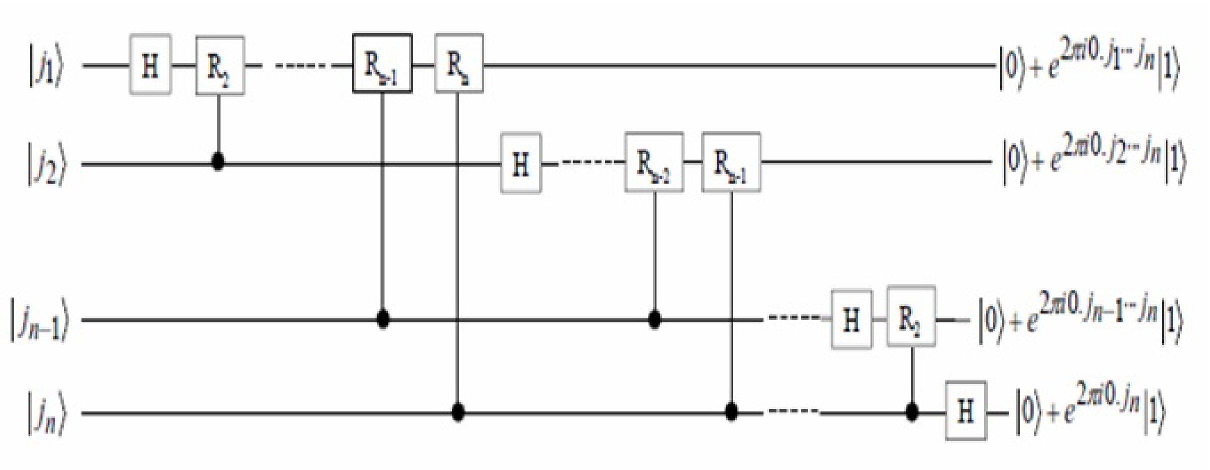
$|j_1\rangle$
H
$R_2$
$R_{n-1}$
$R_n$
$|0\rangle + e^{2\pi i 0.j_1 \cdots j_n}|1\rangle$
$|j_2\rangle$
H
$R_{n-2}$
$R_{n-1}$
$|0\rangle + e^{2\pi i 0.j_2 \cdots j_n}|1\rangle$
$|j_{n-1}\rangle$
H
$R_2$
$|0\rangle + e^{2\pi i 0.j_{n-1} \cdots j_n}|1\rangle$
$|j_n\rangle$
H
$|0\rangle + e^{2\pi i 0.j_n}|1\rangle$

**Figure 2.** Schematic diagram for the quantum Fourier transform.

In this figure, $H$ is a Hadamard gate and $R_k$ is a unitary transformation given by

$$R_k = \begin{bmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^k} \end{bmatrix}.$$

Hence it can be seen that primality testing and integer factorization of an integer $n$ consisted of two primes can be conducted efficiently by using quantum computation besides the notably Shor's integer factorization algorithm (Yang, 2002), which gives us the possibility to break the RSA cryptosystem.

## 4. Conclusion

From the spectrum obtained by the Fourier transform of a correlation function generated from the Riemann zeta function given by $F_n(\omega) = \int_{-\infty}^{+\infty} Z_\sigma\left(t, \frac{1}{2}\log n\right) e^{-i\omega t} dt$, we can see the primarity of an integer $n$ if and only the $F_n(\omega)$ has a single spectra. Moreover we can factorize the integer $n$ consisted of two primes by using this method.

## References

Boashash, B. and P. Black (1987). An efficient real-time implementation of the Wigner - Ville distribution. *Acoustics, Speech and Signal Processing, IEEE Transactions on* **35**(11), 1611–1618.

Dellomo, Michael R. and Garry M. Jacyna (1991). Wigner transforms, Gabor coefficients, and Weyl - Heisenberg wavelets. *The Journal of the Acoustical Society of America* **89**(5), 2355–2361.

Hardy, G.H. and M. Riesz (2005). *The General Theory of Dirichlet's Series*. Cambridge Tracts in Mathematics and Mathematical Physics. Dover Publications.

Kac, M. (1959). *Statistical Independence in Probability, Analysis and Number Theory*. The Carus Mathematical Monographs. Mathematical Association of America.

Musha, T. (2012). A study on the Riemann hypothesis by the Wigner distribution analysis. *JP Journal of Algebra, Number Theory and Applications* **24**(2), 137–147.

Nielsen, M. A. and I. L. Chuang (2000). *Quantum Computation and Quantum Information*. Cambridge Series on Information and the Natural Sciences. Cambridge University Press.

Ribenboim, Paulo (1991). *The Little Book of Big Primes*. Springer-Verlag New York, Inc.. New York, NY, USA.

Rivest, R. L., A. Shamir and L. Adleman (1978). A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM* **21**(2), 120–126.

Yang, S.Y. (2002). *Number Theory for Computiong ($2^{nd}$) Edition*. Springer-Verlag New York, Inc.. New York, NY, USA.

Yen, N. (1987). Time and frequency representation of acoustic signals by means of the wigner distribution function: Implementation and interpretation. *The Journal of the Acoustical Society of America* **81**(6), 1841–1850.