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 5 (2) (2015) 213–220

Primality Testing and Factorization by using Fourier Spectrum of 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 number theory, integer factorization is the decomposition of a composite number into a product of smaller integers, for which there is not known efficient algorithm. In this article, the author tries to make primality testing and factorization of integers by using Fourier transform of a correlation function generated from the Riemann zeta function. From the theoretical analysis, we can see that prime factorization for the integer composed of two different primes can be conducted within a polynomial time and it can be seen that this special case belongs to the P class.

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

1. Introduction

In number theory, integer factorization is the decomposition of a composite number into a product of smaller integers. When the numbers are very large, no efficient, non-quantum integer factorization algorithm is known. However, it has not been proven that no efficient algorithm exists (Klee & Wagon, 1991). The presumed difficulty of this problem is at the heart of widely used algorithms in cryptography such as RSA. Many areas of mathematics and computer science have been brought to bear on the problem, including elliptic curves, algebraic number theory, and quantum computing.

Recently, Shor's algorithm has been proposed by Peter Shor, which is a quantum algorithm for integer factorization. On a quantum computer, it has been proved that Shor's algorithm runs in polynomial time (Shor, 1997). But the polynomial time factoring algorithm of integers has not been found for ordinary computing systems.

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

In optics, we know that white light consists of all visible frequencies mixed together and the prism breaks them apart so we can see the separate frequencies. It is like the Riemann zeta function be consisted of primes shown as

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \frac{1}{(1-p^{-s})}$$

where p runs over all of primes.

From which, we can consider the white light as a zeta function and separate component frequencies are primes. As we use a prism to decompose visible light into components of different frequencies, we can use Fourier transforms as a prism to decompose the zeta function into primes. In this paper, the method of primality testing and prime factorization by using Fourier transforms of the Riemann zeta function is presented.

2. Frequency spectrum of a correlation function generated from the Riemann Zeta function

Riemann zeta function is an analytic function defined by $\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$. From which, we define the Fourier transform of $z_\sigma(t,\tau)$ shown as

$$Z_\sigma(t,\omega) = \lim_{T\to\infty} \int_{-T}^{+T} z_\sigma(t,\tau) e^{-i\omega\tau} d\tau, \tag{2.1}$$

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

$$z_\sigma(t,\tau) = \zeta(\sigma - i(t+\tau/2)) \cdot \zeta^*(\sigma - i(t-\tau/2)). \tag{2.2}$$

In this formula, $\zeta^*(s)$ is a conjugate of $\zeta(s)$.

In the previous paper of author's (Musha, 2014), $Z_\sigma(t,\omega)$ can be shown as

$$Z_\sigma(t,\omega) = \sum_{n=1}^{\infty} \frac{a(n,t)}{n^\sigma} 2\pi\delta(\omega - \tfrac{1}{2}\log n), \tag{2.3}$$

where $a(n,t)$ is a real valued function given by $a(n,t) = \sum_{n=kl} \cos[\log(k/l)t]$ and $\delta(\omega)$ is a Dirac's delta function.

As $a(n,t)$ is a multiplicative on n which satisfies $a(mn,t) = a(m,t)a(n,t)$ for the case when satisfying $(m,n) = 1$, we have the following equation for the integer n given by $n = p^a q^b r^c \cdots$ (Musha, 2012):

$$\begin{aligned} Z_\sigma\left(t, \tfrac{1}{2}\log n\right) = & \frac{2\pi\delta(0)}{n^\sigma} \frac{\sin[(a+1)t\log p]}{\sin(t\log p)} \\ & \cdot \frac{\sin[(b+1)t\log q]}{\sin(t\log q)} \frac{\sin[(c+1)t\log r]}{\sin(t\log r)} \cdots . \end{aligned} \tag{2.4}$$

From the Fourier transform of $Z_\sigma\left(t, \frac{1}{2}\log n\right)$ 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 1. *If $n = p_1 p_2 p_3 \cdots p_k$, where $p_1, p_2, p_3, \cdots, p_k$ are different primes, $F_n(\omega)$ for $\omega > 0$ is consisted of 2^{k-1} discrete spectrum shown as:*

$$F_n(\omega) = 2\pi \sum_{i=1}^{2^k} \delta(\omega - \lambda_{i1} \log p_1 - \lambda_{i2} \log p_2 - \cdots - \lambda_{ik} \log p_k), \tag{2.5}$$

where λ_{ik} equals to -1 or $+1$.

Proof.

As $a(n,t) = \sum_{i=1}^{2^k} [\cos(\lambda_{i1} \log p_1) + \cos(\lambda_{i2} \log p_2) + \cdots\cdots + \cos(\lambda_{ik} \log p_k)]$, where $\log p_1, \log p_2, \log p_3, \cdots, \log p_k$ are linearly independent over $\mathbb{Z}$ (Kac, 1959), thus $F_n(\omega)$ is consisted of 2^{k-1} different spectrum shown as

$$\begin{aligned} F_n(\omega) =& 2\pi \sum_{i=1}^{2^k} \delta(\omega - \lambda_{i1} \log p_1 - \lambda_{i2} \log p_2 - \cdots - \lambda_{ik} \log p_k) \\ &+ 2\pi \sum_{i=1}^{2^k} \delta(\omega + \lambda_{i1} \log p_1 + \lambda_{i2} \log p_2 + \cdots + \lambda_{ik} \log p_k). \end{aligned}$$

□

Then we obtain following Theorems.

Theorem 1. *If and only $F_n(\omega)$ is consisted of a single spectra for $\omega \geq 0$, then n is a prime.*

Proof.

It is clear from Lemma 1. □

Theorem 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 1, 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 $n = p \cdot q$ $(p \neq q)$.

For $r \geq 1$ of the function $a(p^r, t)$:

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

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

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

3. Method for primality testing and factorization by using Fourier spectrum

From Theorems 1 and 2, 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 calculations:

$$\textcircled{1}\quad z_\sigma(t,\tau) = \zeta(\sigma - i(t+\tau/2)) \cdot \zeta^*(\sigma - i(t-\tau/2)), \tag{3.1}$$

$$\textcircled{2}\quad Z_\sigma(t,\omega) = \int_{-\infty}^{+\infty} z_\sigma(t,\tau)e^{-i\omega\tau}d\tau, \tag{3.2}$$

$$\textcircled{3}\quad F_n(\omega) = \int_{-\infty}^{+\infty} Z_\sigma(t, \tfrac{1}{2}\log n)e^{-i\omega t}dt. \tag{3.3}$$

From which we can obtain the Fourier spectrum by $F_n(\omega) = \int_{-\infty}^{+\infty} Z_\sigma(t, \frac{1}{2}\log n)e^{-i\omega t}dt$. Then we can make a primality testing and integer factorization for an integer n, the process of which is shown in Figure 1.

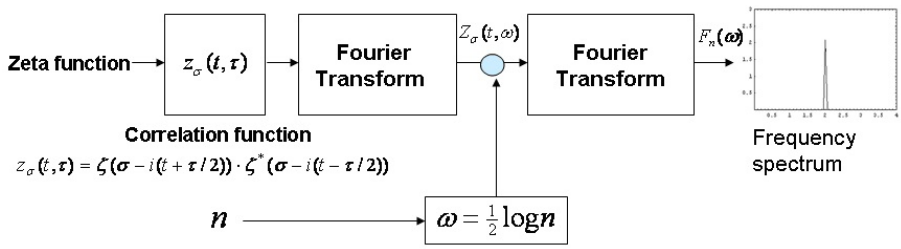

Figure 1. Process to conduct a primality testing for the integer n.

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 $n = p^3$ from Theorem 2.

3.1. Numerical Calculation Method to obtain $F_n(\omega)$

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 $N = [\,8n \log n\,] + 1$.

As Eq.(3.1) can be written in a discrete form as

$$z_\sigma(m,l) = \zeta(\sigma - i(m\Delta t + l\Delta\tau/2)) \cdot \zeta^*(\sigma - i(m\Delta t - l\Delta\tau/2)). \tag{3.4}$$

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

$$z_\sigma(m,l) = \zeta\left(\sigma - i\left(\frac{4\pi n}{N}m + \frac{2\pi n}{N}l\right)\right)\zeta^*\left(\sigma - i\left(\frac{4\pi n}{N}m - \frac{2\pi n}{N}l\right)\right). \tag{3.5}$$

As the total time $T_0 = N \cdot \Delta t = 4\pi n$, then Eq.(3.2) in a discrete form can be given by

$$Z_\sigma(m,k) = \frac{4\pi n}{N}\sum_{l=0}^{N-1} z_\sigma(m,l)\exp[-i2\pi(k\Delta f)\cdot(l\Delta\tau)]. \tag{3.6}$$

At the frequency of $\omega = \frac{1}{2}\log n$, we have

$$k\Delta f \cdot l\,\Delta\tau = \frac{\log n}{4\pi} \times \frac{\pi}{2\log n}\,l = \frac{l}{8}, \tag{3.7}$$

then we have

$$y(m) = \frac{4\pi n}{N}\sum_{l=0}^{N-1} z_\sigma(m,l)\exp\left(-i\frac{\pi}{4}l\right), \tag{3.8}$$

which corresponds to $Z_\sigma\left(t, \frac{1}{2}\log n\right)$.

From which, we have the discrete form of Eq.(3.3) given by

$$Y(k) = \frac{4\pi n}{N}\sum_{m=0}^{N-1} y(m)\exp\left(-i2\pi\frac{km}{N}\right), \tag{3.9}$$

which shows the spectrum of $F_n(\omega)$.

Thus we need the following three steps for calculations to obtain $F_n(\omega)$.

① Input the integer n and we let $N = [\,8n\log n\,] + 1$,

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

③ For $m = 0 \sim N-1$, calculate $y(m) = \frac{4\pi n}{N}\sum_{l=0}^{N-1} z_\sigma(m,l)\exp\left(-i\frac{\pi}{4}l\right)$,

④ For $k = 0 \sim N-1$, calculate $Y(k) = \frac{4\pi n}{N}\sum_{m=0}^{N-1} y(m)\exp\left(-i2\pi\frac{km}{N}\right)$.

3.2. Some examples of primality testing

To confirm the validity of discrete computational algorism given in this paper, we try to compute some examples shown as follows:

To generate the Riemann zeta function, we use Mathematica by Wolfram Research.

At the calculation, we set $\sigma = 1.1$ to compute $F_n(\omega)$ to minimize the noise generated by DFT calculations.

(Calculation program by using Mathematica).

```
σ=1.1; (Real Part of Zeta function)
n0=17; (Input an Integer)
n1=Ceiling[8*n0*Log[n0]];(Element number for calculation)
x[m_,l_]:=Zeta[σ-I*(4*Pi*n0*m/n1+2*Pi*n0*l/n1)]*
Conjugate [Zeta[σ-I*(4*Pi*n0*m/n1-2*Pi*n0*l/n1)]];(Autocorrelation function of
zeta function)
data=Table[N[4*Pi*n0/n1*Sum[x[m,l]*Exp[-I*Pi*l/4],{l,0,n1 -1}]],{m,0,n1-1}];
ListPlot[Abs[InverseFourier[data]],PlotJoined→True,PlotR
ange→{{0,n1/2}, {0,200}}, Frame→True]; (DFT calculation and plot results)
```

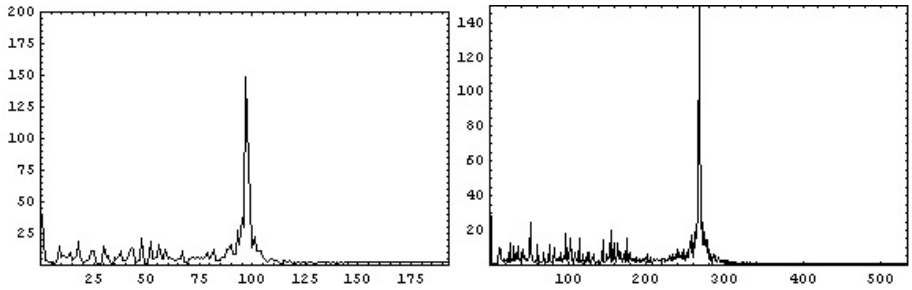

Figure 2. Computational result for n=17(left) and n=37(right).

From calculation, we can see that there exists only one spectrum at the center and it can be shown that both of numbers, 17 and 37 are primes.

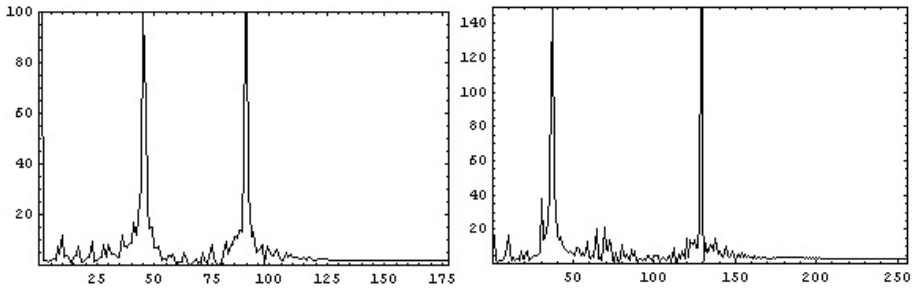

Figure 3. Computational result for n=16(left) and n=21(right).

These results corresponds to $a(p^4, t) = 1 + 2\cos(2t \log p) + 2\cos(4t \log p)$ (three spectrum including $\omega = 0$) and $a(p \cdot q, t) = \cos[(\log q - \log p)t] + \cos[(\log q - \log p)t]$ (two spectrum), and we can see that they are composite numbers.

4. Running time for prime factorization by using DFT algorithms

As the value of Riemann zeta function can be generated by the formula (Gourdon & Sebah, 2003)

$$\zeta(s) = \frac{1}{d_0(1-2^{1-s})}\sum_{k=1}^{m}\frac{(-1)^{k-1}d_k}{k^s} + \gamma_m(s), \tag{4.1}$$

where $d_k = m\sum_{j=k}^{m}\frac{(m+j-1)!\,4^j}{(m-j)!\,(2j)!}$, we can compute $\zeta(\sigma+it)$ with d decimal digits of accuracy, which requires number of term m roughly equal to $m \approx 1.3d + 0.9|t|$ (Gourdon & Sebah, 2003).

To calculate Eq.(3.4), we need to compute up to $t = N\cdot\Delta t = 4\pi n$, hence we need $m \approx 1.3d + 3.6\pi n$ to obtain the value of $\zeta(\sigma+it)$ with d decimal digits of accuracy, which has expected running time $O(n^2)$.

As the running time to require DFT calculation is $O(N^2)$, thus we need the running time to complete calculations of steps from ① to ④, to be estimated as $O(n^2(\log n)^2)$. Hence it can be seen that primality testing of integer can be conducted in a polynomical time by using this algorithm.

Moreover, we can factor the integer which is composed of two different primes by steps from ① to ④, because the calculated result of $F_n(\omega)$ has only two spectrum according to Theorem 2.

As two spectrum obtained can be given by $\omega_1 = \log q - \log p$ and $\omega_2 = \log q + \log p$ (Musha, 2014), we obtain $p = \sqrt{n\cdot\exp(-\omega_1)}$ and $q = \sqrt{n\cdot\exp(\omega_1)}$ $(q > p)$ from them if we let ω_1 is a small spectrum obtained from the calculation of $F_n(\omega)$. From these obtained values for p and q, we have finally to examine whether they satisfy $n = p\cdot q$ or not.

Thus it can be seen that prime factorization for the integer composed of two different primes can be conducted in a polynomial time. There is no efficient, non-quantum integer factorization algorithm is not known now (Yang, 2002), and it has been widely believed that no algorithm is existed that can factor all integers in polynomial time. Thus the presumed difficulty of this problem is at the heart of widely used algorithms in cryptography such as RSA. Contrary to this, we can see that prime factorization for the integer composed of two different primes can be conducted within a polynomial time and it can be shown that this special case belongs to the P class from the theoretical analysis.

However, the validity of this factoring algorithm has been confirmed for only small integers by the restriction of a computer capacity and hence it is necessary to confirm the validity of this algorithm for large integers by using more powerful computer systems.

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 a integer n if and only the $F_n(\omega)$ has a single spectra for $\omega \geq 0$. Furthermore, it can be shown that the prime factorization can be conducted within a polynomial time for the special case that the integer is composed of two different primes and hence we can conclude that that prime factorization for the integer composed of two different primes is in the P class.

References

Gourdon, X. and P. Sebah (2003). Numerical evaluation of the Riemann Zeta-function. http://numbers.computation.free.fr/Constants/Miscellaneous/zetaevaluations.pdf.

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

Klee, V. and S. Wagon (1991). *Old and new unsolved problems in plane geometry and number theory*. The Mathematical Association of America.

Musha, Takaaki (2012). A study on the Riemann hypothesis by the Wigner distribution analysis.. *JP J. Algebra Number Theory Appl.* **24**(2), 137–147.

Musha, Takaaki (2014). Primality 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* **4**(2), 185–191.

Shor, P. W. (1997). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.* **26**(5), 1484–1509.

Yang, S. Y. (2002). *Number Theory for Computiong (2nd Edition)*. Springer-Verlag, New York.

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.