An integral representation of divisor function.
An equation for prime numbers.

Kholupenko E.E.

Ioffe Physical-Technical Institute, St.-Petersburg 194021, Russia

Abstract

A representation of divisor function $\tau(n) \equiv \sigma_0(n)$ by means of logarithmic residue of a function of complex variable is suggested. This representation may be useful theoretical instrument for further investigations of properties of natural numbers.

1   Introduction

Properties of natural numbers are the fundamental question of mathematics. Investigations of these properties in the Ancient Times (e.g. the infinitude of prime numbers which was shown by Euclid, Sieve of Eratosthenes for prime numbers, consideration of Diophantine equations) led to the birth of elementary theory of numbers. Later investigations (e.g. Fermat's Last theorem, investigations of zeta-function by Euler and Riemann) have led to the development the great branch of mathematics - the analytical theory of numbers. The important problems of modern number theory are the problems of effective search of prime numbers and complexity (and factorization) or primality of arbitrary natural number. Today essential efforts are applied for consideration of these questions: many fast methods for factorization (e.g. Pollard ρ-algorithm [1], elliptic curve method [2], quadratic sieve algorithm [3], general number field sieve [4]) and tests of primality (e.g. Miller-Rabin test [5], Lucas-Lehmer test [6], AKS test [7]) are developed, projects on search of large prime numbers are running (GIMP [8], PrimeGride [9], Seventeen or Bust [10] and others), databases of prime numbers are updated (e.g. The List of Largest Known Primes [11], OEIS [12]). Such interest is due to not only desire to understand the nature of numbers and to resolve some fundamental problems of mathematics but also due to opportunity of practical application of properties of natural numbers, e.g. for the cryptographic systems with public key (for example RSA [13]), hash-tables, and generation of pseudorandom numbers (e.g. Mersenne twister [14]).

The aim of this paper is to suggest a theoretical instrument for investigation of quantity of divisors of natural number, which may be useful for further investigations of properties of natural numbers.

2   Integral representation of divisor function

Main idea is similar to the one of method of trigonometric sums [15]. Using the fact that $\exp\left(2\pi i x\right)$ equals unity only for integer value of real number x one may say that function:

$$f_s(x) = \exp\left(2\pi i x\right) + \exp\left(2\pi i s/x\right) - 2 \tag{1}$$

has zeros only for values of x which are divisors of natural number s (we will denote these numbers as x_j^s, where superscript s highlights dependence on natural number s, subscript j denotes integer sequence number of corresponding zero). Note that

$$\exp\left(2\pi i x_j^s\right) = 1, \quad \exp\left(2\pi i s/x_j^s\right) = 1 \tag{2}$$

Unfortunately, direct use of $f_s(x)$ (e.g. search of global minima of $f_s(x)$ by using numerical iteration methods) for factorization of natural number s or for counting number of divisors of s is almost impossible because of frequent oscillations of function $f_s(x)$ (see fig. 1).

Number of zeros of this function in the interval $[1; s]$ gives us the number of divisors of s. To count the number of zeros of f_s one can use logarithmic residue of f_s. In general case the logarithmic residue is the following (e.g. [16]):

$$\gamma\left[f, L\right] = \frac{1}{2\pi i} \int_L \frac{f'\left(z\right) dz}{f\left(z\right)} = N_f - P_f \tag{3}$$

2

where f is a function of complex number z, L is a closed contour on the complex plane $\mathbb{C}$, N_f is the number of zeros of function f within the contour L (taking into account the orders of zeros), P_f is the number of poles of function f within the contour L (taking into account the orders of poles). If function f has no poles within contour L (e.g. f is the smooth functionof z) then one may write:

$$\gamma\,[f, L] = \sum_{z_j \in \mathbb{L}: f(z_j)=0} k_i \tag{4}$$

where $\mathbb{L}$ is the field within the contour L (i.e. $\mathbb{L}$ is the field limited by the contour L on the complex plane $\mathbb{C}$), z_j are zeros of function f in the field $\mathbb{L}$, k_j is the order of zero z_j, i.e. in the vicinity of z_j the function $f(z)$ can be presented as

$$f(z) = \frac{f^{(k_j)}(z_j)}{k_j!}(z - z_j)^{k_j} + O\left((z - z_j)^{k_j+1}\right) \tag{5}$$

Using (4) one can construct the expression for counting number of zeros of function $f_s(z)$ in the interval $[1; \sqrt{s}]$. Let us define the following functions:

$$\tau_-(s) = \gamma\left[f_s, L_s^-\right], \qquad \tau_c(s) = \gamma\left[f_s, L_s^c\right], \qquad \tau_+(s) = \gamma\left[f_s, L_s^+\right] \tag{6}$$

where L_s^- is the contour given (e.g.) by the following points z (see fig. 2):

$$\begin{aligned}
z &= 1 - \epsilon + iy, \quad y \in [-\epsilon; +\epsilon] \\
x &+ i\epsilon, \quad x \in \left[(1 - \epsilon); \left(\sqrt{s} - \epsilon\right)\right] \\
&\left(\sqrt{s} - \epsilon\right) + iy, \quad y \in [+\epsilon; -\epsilon] \\
x &- i\epsilon, \quad x \in \left[\left(\sqrt{s} - \epsilon\right); (1 - \epsilon)\right]
\end{aligned} \tag{7}$$

L_s^c is the contour given (e.g.) by the following points z (see fig. 2):

$$\begin{aligned}
z &= \sqrt{s} - \epsilon + iy, \quad y \in [-\epsilon; +\epsilon] \\
x &+ i\epsilon, \quad x \in \left[\left(\sqrt{s} - \epsilon\right); \left(\sqrt{s} + \epsilon\right)\right] \\
&\left(\sqrt{s} + \epsilon\right) + iy, \quad y \in [+\epsilon; -\epsilon] \\
x &- i\epsilon, \quad x \in \left[\left(\sqrt{s} + \epsilon\right); \left(\sqrt{s} - \epsilon\right)\right]
\end{aligned} \tag{8}$$

L_s^+ is the contour given by the following points z (see fig. 2):

$$\begin{aligned}
z &= 1 - \epsilon + iy, \quad y \in [-\epsilon; +\epsilon] \\
x &+ i\epsilon, \quad x \in \left[(1 - \epsilon); \left(\sqrt{s} + \epsilon\right)\right] \\
&\left(\sqrt{s} + \epsilon\right) + iy, \quad y \in [+\epsilon; -\epsilon] \\
x &- i\epsilon, \quad x \in \left[\left(\sqrt{s} + \epsilon\right); (1 - \epsilon)\right]
\end{aligned} \tag{9}$$

where ϵ is the positive real number. Parameter ϵ should be small enough to exclude zeros z_j^s (z_j^s denote zeros of $f_s(z)$ in complex plane) which do not lie on the real axis. Note that $\tau_+(s) = \tau_-(s) + \tau_c(s)$.

3

Studying values of $\tau_-(s)$, $\tau_c(s)$ and $\tau_+(s)$ one should calculate the orders of zeros z_j^s which lie on the real axis (i.e. $z_j^s = x_j^s$). This demands calculation of derivative of $f_s(z)$:

$$f_s'(z) = 2\pi i \left[\exp(2\pi i z) - \frac{s}{z^2} \exp\left(\frac{2\pi i s}{z}\right)\right] \tag{10}$$

Taking into account (2) one may write

$$f_s'(x_j^s) = 2\pi i \left[1 - \frac{s}{\left(x_j^s\right)^2}\right] \tag{11}$$

Thus $f_s'(x_j^s) \neq 0$ for $x_j^s \in [1; \sqrt{s})$, and therefore all zeros x_j^s in interval $[1; \sqrt{s})$ have order which equals unity. If $\sqrt{s}$ is also divisor of s then one should investigate the order of this zero. From (11) it is evident that this order is not equal unity. Thus one should find the second order of $f_s(z)$:

$$f_s''(z) = 2\pi i \left[2\pi i \exp(2\pi i z) + \frac{2s}{z^3} \exp\left(\frac{2\pi i s}{z}\right) + 2\pi i \frac{s^2}{z^4} \exp\left(\frac{2\pi i s}{z}\right)\right] \tag{12}$$

If the value $\sqrt{s}$ is an integer number (this case is interesting for us) then one may write:

$$f_s''\left(\sqrt{s}\right) = -8\pi^2 + 4\pi i s^{-1/2} \neq 0 \tag{13}$$

Expression (13) means that the order of zero in point $\sqrt{s}$ equals 2 (if $\sqrt{s}$ is integer and divisor of number s) or 0 (if $\sqrt{s}$ is not integer and not a zero of function $f_s(z)$), i.e. $\tau_c(s) = 0$ or 2.

Knowledge of behaviour of functions $\tau_-(s)$, $\tau_c(s)$ and $\tau_+(s)$ allows us to calculate the number of divisors $\tau(s)$ of integer number s. Taking into account symmetry of quantity of divisors of s relative to the number $\sqrt{s}$ one may write:

$$\tau(s) = 2\tau_-(s) + \frac{1}{2}\tau_c(s) = \frac{3}{2}\tau_-(s) + \frac{1}{2}\tau_+(s) = 2\tau_+(s) - \frac{3}{2}\tau_c(s) \tag{14}$$

Explicit expressions for $\tau_-(s)$, $\tau_c(s)$ and $\tau_+(s)$ are the following:

$$\tau_-(s) = \int_{L_s^-} \frac{\exp(2\pi i z) - (s/z^2)\exp(2\pi i s/z)}{\exp(2\pi i z) + \exp(2\pi i s/z) - 2} dz \tag{15}$$

$$\tau_c(s) = \int_{L_s^c} \frac{\exp(2\pi i z) - (s/z^2)\exp(2\pi i s/z)}{\exp(2\pi i z) + \exp(2\pi i s/z) - 2} dz \tag{16}$$

$$\tau_+(s) = \int_{L_s^+} \frac{\exp(2\pi i z) - (s/z^2)\exp(2\pi i s/z)}{\exp(2\pi i z) + \exp(2\pi i s/z) - 2} dz \tag{17}$$

3 Prime number equation

One of the interesting cases of using representation (14-17) appears when s is a prime number. In this case $\tau(s) = 2$ and one can write the equation for prime numbers using equivalent condition $\tau_+(s) = 1$. To prove the equivalence of $\tau(s) = 2$ and $\tau_+(s) = 1$ let

4

us consider the following:

1) From $\tau(s) \geq 2$ and $\tau(s) \leq 2\tau_+(s)$ (from (14)) one can show that $\tau_+(s) = 1 \Rightarrow \tau(s) = 2$,

2) From $\tau_+(s) \geq 1$, $\tau_+(s) \neq 2$, and $\tau_+(s) \leq \tau(s)$ one can show that $\tau(s) = 2 \Rightarrow \tau_+(s) = 1$.

Thus one can write the following equation for prime numbers p:

$$\int_{L_p^+} \frac{\exp\left(2\pi i z\right) - (p/z^2)\exp\left(2\pi i p/z\right)}{\exp\left(2\pi i z\right) + \exp\left(2\pi i p/z\right) - 2}dz = 1 \tag{18}$$

4   Conclusion

Formulae (14-17) for an integral representation of divisor function and equation (18) for prime numbers have been shown in the present paper. Unfortunately the calculation of expressions (14-17) and (18) for the typical values of s and p (which are needed in practical problems) demands huge computational time and resources. Thus direct application of formulae (14-17) and (18) is impossible. Nevertheless, these formulae may be useful for further investigations of properties of natural numbers and solving of practical and fundamental problems of number theory such as construction of new tests of primality and proof of the infinitude of twin primes.
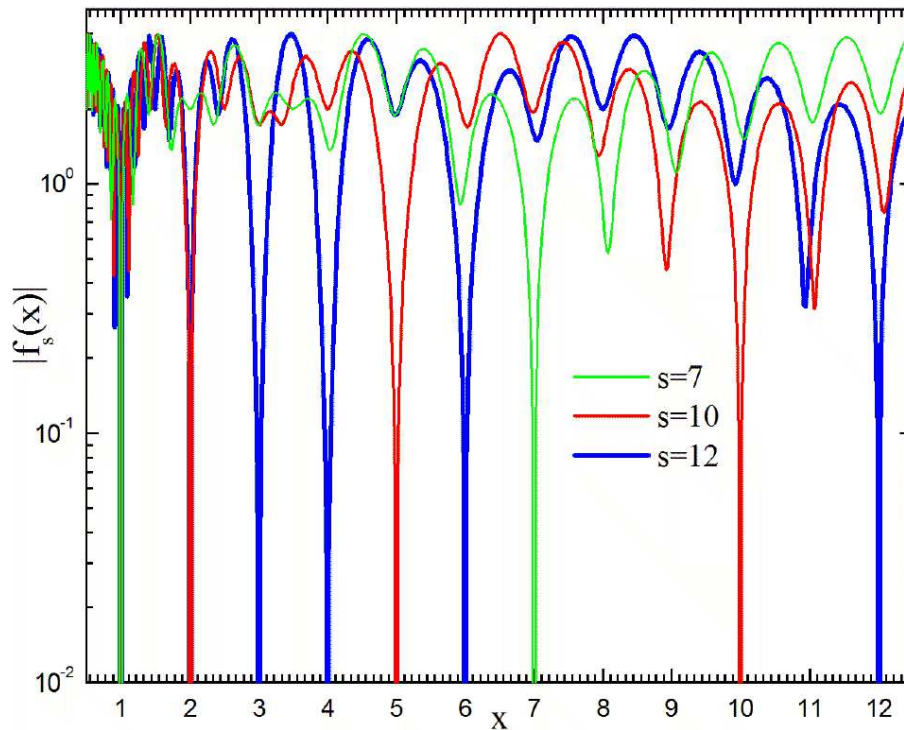
Figure 1: Dependence of module of function $f_s(x)$ on real variable x.

References

[1] Pollard J. M., BIT Numerical Mathematics 15 (3): 331 - 334 (1975)

[2] Lenstra Jr. H. W., Annals of Mathematics 126 (2): 649 - 673 (1987)

[3] Pomerance C., Computational Methods in Number Theory, Part I, Lenstra Jr. H.W. and Tijdeman R., eds., Math. Centre Tract 154, Amsterdam, pp 89-139 (1982)

[4] Kleinjung T., Mathematics of Computation 75 (256): 2037 - 2047 (2006)

[5] Rabin M. O., Journal of Number Theory 12 (1): 128 - 138 (1980)

[6] Lehmer D. H., Annals of Mathematics, 31, 419 - 448 (1930)

[7] Agrawal M., Kayal N., Saxena N., Annals of Mathematics 160 (2): 781 - 793 (2004)

[8] Great Internet Mersenne Prime Search, http://www.mersenne.org/
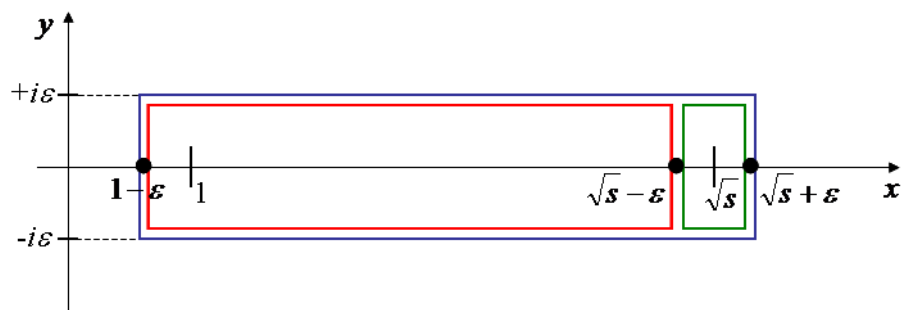
[9] http://www.primegrid.com/

Figure 2: Examples of contours L in complex plane for calculation of logarithmic residue of function $f_s(x)$.

[10] http://www.seventeenorbust.com/

[11] Caldwell, C. K., The List of Largest Known Primes, http://primes.utm.edu/primes/

[12] The On-Line Encyclopedia of Integer Sequences, http://oeis.org/

[13] Rivest R., Shamir A., Adleman L., Communications of the ACM 21 (2): 120 - 126 (1978)

[14] Matsumoto M., Nishimura T., ACM Trans. on Modeling and Computer Simulations 8 (1): 3-30 (1998)

[15] Vinogradov I.M., "The method of trigonometric sums in the theory of numbers" , Interscience (1954) (Translated from Russian)

[16] Goncharov V. L., Teoriya funkcij kompleksnogo peremennogo ("The theory of functions of complex variable"), in russian, publishing company "Prosveschenie", Moscow (1955)