韓國컴퓨터情報學會 論文誌
第16卷 第10號, 2011. 10.

2011-16-10-3-1

소수계량함수

이 상 운*・ 최 명 복 **

The Prime Counting Function

Sang-Un, Lee * ・Myeong-Bok, Choi **

요 약

리만의 제타함수 $\zeta(s)$는 주어진 수 x보다 작은 소수의 개수 $\pi(x)$를 구하는 해답으로 알려져 있으며, 소수정리에서 지금까지 리만의 제타 함수 이외에 $\frac{x}{\ln x}$, $Li(x)$와 $R(x)$의 근사치 함수가 제안되었다. 여기서 $\pi(x)$와의 오차는 $R(x) < Li(x) < \frac{x}{\ln x}$이다. 로그적분함수 $Li(x) = \int_2^x \frac{1}{\ln t} dt$, $\sim \frac{x}{\ln x} \sum_{k=0}^{\infty} \frac{k!}{(\ln x)^k} = \frac{x}{\ln x}(1 + \frac{1!}{(\ln x)^1} + \frac{2!}{(\ln x)^2} + \cdots)$이다. 본 논문은 $\pi(x)$는 유한급수 $Li(x)$로 표현됨을 보이며, 일반화된 $\sqrt{\alpha x} \pm \beta$의 소수계량함수를 제안한다. 첫 번째로, $\pi(x)$는 $0 \le t \le 2k$의 유한급수인 $Li_3(x) = \frac{x}{\ln x}(\sum_{t=0}^{\alpha} \frac{k!}{(\ln x)^k} \pm \beta)$와 $Li_4(x) = \left\lfloor \frac{x}{\ln x}(1 + \alpha \frac{k!}{(\ln x)^k} \pm \beta) \right\rfloor$, $k \ge 2$ 함수로 표현됨을 보였다. $Li_3(x)$는 $\pi(x) \simeq Li_3(x)$가 되도록 α 값을 구하고 오차를 보정하는 β 값을 갖도록 조정하였다. 이 결과 $x = 10^k$에 대해 $Li_3(x) = Li_4(x) = \pi(x)$를 얻었다. 일반화된 함수로 $\pi(x) = \sqrt{\alpha x} \pm \beta$를 제안하였다. 제안된 $\pi(x) = \sqrt{\alpha x} \pm \beta$ 함수는 리만의 제타함수에 비해 소수를 월등히 계량할 수 있었다.

▸ Keywords : 소수 정리, 소수계량함수, 리만 제타함수, 자연로그함수, 옵셋 로그적분함수

Abstract

The Riemann's zeta function $\zeta(s)$ has been known as answer for a number of primes $\pi(x)$ less than given number x. In prime number theorem, there are another approximation function $\frac{x}{\ln x}$, $Li(x)$, and $R(x)$. The error about $\pi(x)$ is $R(x) < Li(x) < \frac{x}{\ln x}$. The logarithmic integral function is $Li(x) = \int_2^x \frac{1}{\ln t} dt \sim \frac{x}{\ln x} \sum_{k=0}^{\infty} \frac{k!}{(\ln x)^k} = \frac{x}{\ln x}(1 + \frac{1!}{(\ln x)^1} + \frac{2!}{(\ln x)^2} + \cdots)$. This paper shows that the $\pi(x)$ can be represent with finite $Li(x)$, and presents generalized prime counting function $\sqrt{\alpha x} \pm \beta$. Firstly, the $\pi(x)$ can be represent to $Li_3(x) = \frac{x}{\ln x}(\sum_{t=0}^{\alpha} \frac{k!}{(\ln x)^k} \pm \beta)$ and $Li_4(x) = \left\lfloor \frac{x}{\ln x}(1 + \alpha \frac{k!}{(\ln x)^k} \pm \beta) \right\} k \ge 2$ such that $0 \le t \le 2k$. Then, $Li_3(x)$ is adjusted by $\pi(x) \simeq Li_3(x)$ with α and error compensation value β. As a results, this paper get the

• 제1저자 : 이상운*, 교신저자 : 최명복**
• 투고일 : 2011. 05. 13, 심사일 : 2011. 06. 08, 게재확정일 : 2011. 07. 25.
*, ** 강릉원주대학교 멀티미디어공학과 (Dept. of Multimedia Science, Gangneung-Wonju National University)

$Li_3(x) = Li_4(x) = \pi(x)$ for $x = 10^k$. Then, this paper suggests a generalized function $\pi(x) = \sqrt{\alpha x} \pm \beta$. The $\pi(x) = \sqrt{\alpha x} \pm \beta$ function superior than Riemann's zeta function in representation of prime counting.

▸ Keywords : prime number theorem, Riemann zeta function, natural logarithmic function, offset logarithmic integral function

I. 서 론

1과 자신 이외의 어떤 수로도 나눌 수 없는 수, 즉 소수 (prime number)는 암호체계 (cryptograph)에 널리 활용되고 있다[1]. RSA 암호체계의 공개키 $n = pq$를 생성하기 위해서는 2개 소수 p,q를 임의로 선택하여 곱한 결과를 쉽게 얻는다. 이 합성수 n을 반소수 (semiprime)라고도 한다. 여기서 임의로 선택한 p,q가 소수인지 여부는 소수 판별법 (primality test, PT)을 적용한다. 또한, RSA 암호 해독은 반소수 n을 p,q로 소인수분해해야 하지만 쉽지가 않다. 따라서 공개키를 만들기는 쉬운 반면에 역으로 이를 해독하는 소인수 분해는 어렵다는데 기반하여 RSA 암호체계가 개발되었으며, 이를 일방향함수 (one-way function)라고도 한다.

고대 그리스의 에라토스테네스 (BC. 278 ~ BC. 195)가 소수를 구하는 방법인 에라토스테네스 체 (Sieve of Erathosthenes)를 처음으로 제시하였다[2]. 이 방법은 $[2,n]$의 자연수를 나열하고 $[2, \sqrt{n}]$에 대해 배수를 삭제하면 남은 수가 n보다 작은 소수의 개수이다. 이후 1859년에 리만은 "주어진 수 n보다 작은 소수의 개수에 관하여"란 논문에서 제타 함수 (zeta function)를 제안하고 $2,3,5,7,\cdots$의 소수들은 어떤 불규칙한 배열 패턴을 지니고 있는데도 불구하고 $\zeta(0)$의 직선상에 존재한다고 제시하였다[3]. 리만 가설이란 "$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \cdots$의 복소수 자명하지 않은 근 $s = a + bi (i = \sqrt{-1})$의 실수부 a,b는 모두 $\frac{1}{2}$이다."[4]. 소수의 분포 패턴을 하나의 함수로 제시한 리만 가설이후 150년 동안 리만 가설은 증명되지 못하고 있다. 리만 가설을 증명할 수 있다면 클레이 수학재단 (Clay Mathematics Institute)에서 제시한 상금 $1,000,000를 획득할 수 있다.

소수의 정확한 규칙 (분포 패턴)은 지금까지 밝혀지지 않고 있다. 소수 정리 (prime number theorem)는 소수의 근사적인 분포에 관한 정리로 소수가 어떻게 분포되어 있는지를 개략적으로 표현해준다[1]. 지금까지 알려진 소수의 정리는 주어진 수 x보다 작은 소수의 개수를 소수계량함수 (prime- counting function) $\pi(x)$라 할 때 $\pi(x) \sim \frac{x}{\ln x}$라는 소수분포의 근사적 법칙이다. 또한 Gauss는 옵셋 로그 적분 함수 (offset logarithmic integral function) $Li(x) = \int_2^x \frac{1}{\ln t} dt \sim \frac{x}{\ln x} \sum_{k=0}^{\infty} \frac{k!}{(\ln x)^k}$를 제시하였다. 리만 가설은 $\pi(x) \sim Li(x) = \int_0^x \frac{1}{\ln x} dx$를 고찰하기 위해 $\zeta(s)$와 리만 소수계량함수 $R(x)$를 제안하였다. $\pi(x)$와의 오차는 $R(e) < Li(x) < \frac{x}{\ln x}$ 형태를 나타내고 있으며, $R(x)$가 $\pi(x)$에 가장 근사한 값을 얻고 있다[1,5]. 그러나 아직까지도 $\pi(x)$의 정확한 값을 추정하는 함수는 제시되지 않고 있다.

소수 정리의 증명은 리만 제타함수에 대해 복소해석법을 사용하는 방법을 해석적 증명 (analytic proof), 복소해석법을 사용하지 않고 증명하는 방법을 초등적 증명 (elementary proof)이라 한다[5]. 대부분의 수학자들은 오랫동안 복소해석학을 사용하지 않고 소수정리를 증명할 방법이 없다고 생각하였다.

본 논문의 초점은 "소수 정리 $\pi(x)$를 구하는데 있어서 리만 제타함수 $\zeta(s)$ 이외에 어떠한 다른 함수가 존재하는가?"이다. 2장에서는 소수 정리와 관련된 연구를 고찰한다. 3장에서는 $\pi(x)$를 근사적으로 표현하지 않고 정확히 표현하는 함수를 제시한다.

II. 소수정리 관련 연구

$\pi(x)$의 정확한 값은 전수탐색 (Exhaustive or Brute-Force Search)방법으로 $2^p - 1$회, 즉 $O(2^p)$를 수행해야 하며, 포함-배제 원칙 (inclusive-exclusive principle)을 적용하여 식 (1)로 구할 수 있으나 이는 하노이 타워 (Hanoi Tower)의 수행횟수와 동일하여 비현실적이다. 포함-배제 원칙을 변형시킨 소수계량함수로는 Legendre, Lehmer, Mapes와

Meissel 공식이 있다[5].

$$\pi(x)=[(x-1)+|p_i|]-\Sigma\left|\left\lfloor \frac{x}{p_i}\right\rfloor\right|+\Sigma\left|\left\lfloor \frac{x}{p_ip_j}\right\rfloor\right|-\Sigma\left|\left\lfloor \frac{x}{p_ip_jp_k}\right\rfloor\right|+\Sigma\left|\left\lfloor \frac{x}{p_ip_jp_kp_l}\right\rfloor\right|-\cdots \quad (1)$$

예로, $x=100$에 대해 고찰해 보자.

$x=100$, $\lfloor \sqrt{x} \rfloor=10$, $p=2,3,5,7$, $|p|=4$, $2^4-1=15$ 회

x	x/p	x/pq	x/pqr	$x/pqrs$
2	100/2=50	2*3=6: 100/6=16	2*3*5=30: 100/30=3	2*3*5*7=210: 0
3	100/3=33	2*5=10: 100/10=10	2*3*7=42: 100/42=2	
5	100/5=20	2*7=14: 100/14=7	2*5*7=70: 100/70=1	
7	100/7=14	3*5=15: 100/15=6	3*5*7=105: x	
		3*7=21: 100/21=4		
		5*7=35: 100/35=2		
4	117	45	6	0

$\pi(x)=(99+4)-117+45-6=(103-117+39)=(-14+39)=25$

주어진 수 x보다 작은 소수의 개수 $\pi(x)$에 관한 소수 정리는 $\pi(x)\sim\frac{x}{\ln x}$라는 소수분포의 점근적 법칙이다. 이 소수 분포에 대해 1796년에 Legendre는 $\pi(x)\sim\frac{x}{\ln x-B}$, $B=1.08366$의 변형을 제시하였다[6]. 또한 Gauss는 보다 좋은 근사 공식으로 $Li(x)=\int_2^x \frac{1}{\ln t}dt$을 제시하였으며, 근사적 확장을 하면 식 (2)가 된다[1,7].

$$Li(x)\sim\frac{x}{\ln x}\sum_{k=0}^{\infty}\frac{k!}{(\ln x)^k}$$
$$=\frac{x}{\ln x}\left(1+\frac{1!}{(\ln x)^1}+\frac{2!}{(\ln x)^2}+\frac{3!}{(\ln x)^3}+\cdots\right) \quad (2)$$

식 (2)는 $\pi(x)$를 잘 표현하는 반면에, 이 식도 무한급수 형태로 계산은 쉽지 않다.

리만의 제타함수 값 $\zeta(0)$이 되는 변수들은 직선상에 존재한다. 제타함수와 소수를 연관시킨 방법은 오일러가 식 (3)을 제안하였다[1,8]. 이 함수는 임의로 선택한 정수들 s가 서로소 (coprime)일 확률을 계산하는데 사용된다. 직관적으로 소수 p로 나누어질 수 있는 어떤 수의 확률은 p^{-1}이다. 따라서 정수들 s가 이 소수로 나누어질 수 있는 확률은 p^{-s}, 나누어질 수 없는 확률은 $1-p^{-s}$이다.

$$\zeta(s)=\sum_{n=1}^{\infty}\frac{1}{n^s}=\prod_p^{\infty}(1-p^{-s})^{-1}=\left(\prod_p^{\infty}\frac{1}{1-p^{-s}}\right)^{-1}=\frac{1}{\zeta(s)}$$
$$=\left(1-\frac{1}{2^s}\right)\left(1-\frac{1}{3^s}\right)\left(1-\frac{1}{5^s}\right)\left(1-\frac{1}{7^s}\right)\cdots (3)$$

식 (3)을 만족시키려면 무한급수로 존재하는 모든 소수에 대해 계산해야한다.

리만의 소수계량함수 $R(x)$는 $R(x)=Li(x)-\sum_{\rho}Li(x^{\rho})-\mathrm{Ln}(2)+\int_x^{\infty}\frac{1}{t(t^2-1)\ln t}dt = \sum_{n=1}^{\infty}\frac{1}{n}\mu(n)Li(x^{\frac{1}{n}}) \sim Li(x)-\frac{1}{2}Li(x^{\frac{1}{2}})-\frac{1}{3}Li(x^{\frac{1}{3}})-\frac{1}{5}Li(x^{\frac{1}{5}})+\frac{1}{6}Li(x^{\frac{1}{6}})-\frac{1}{7}Li(x^{\frac{1}{7}})+\cdots$로 알려져 있다. 여기서, ρ는 리만 제타함수 $\zeta(s)$의 모든 자명하지 않은 0 값 ρ를 모두 합한 값이며, $\mu(n)$은 Möbius 함수이다.

Wikipedia[1]와 Mathworld[5]에서 제시한 $\pi(x)$와 $\frac{x}{\ln x}$, $Li(x)$, $R(x)$에 대해 $\pi(x)$와의 오차는 표 1에 제시되어 있다.

<표 1>의 데이터와 Legendre와 유사한 공식을 적용하여 $\pi(x)$와의 오차를 계산하였다. 그 결과 $R(x)<Li(x)<\frac{x}{\ln x-1.0297}<\frac{x}{0.98074\ln x}<\frac{x}{\ln x-1.08366}<\frac{1.00001x}{\ln x}<\frac{x}{\ln x}$를 보였다. 즉, $\frac{x}{\ln x}$는 $\pi(x)$보다 적은 값을, $Li(x)$는 $\pi(x)$를 초과한 값을 보이고 있다. 반면에 $R(x)$가 $\pi(x)$에 가장 근사한 값을 얻고 있다. 결국, $\pi(x)$를 정확히 표현하는 공식은 아직 제시되지 않고 있다.

10^k 단위로 소수의 개수를 구한 <표 1>을 선택한 이유는 RSA 수 $n=pq$의 경우, n의 자리수 $l(n)=$짝수라면 $l(p)=l(q)=l(n)/2$이므로 p,q는 동일한 10^k 범위에서 임의로 선택한 소수가 되기 때문이다. 예로, $1933\times9419=18206927$인 경우 $l(n)=8, l(p)=l(q)=4$이다. 즉, p,q는 $10^4=[1001,9999]$에서 선택되었다.

Wikipedia[1]가 제시한 <표 1>의 $Li(x)$로 계산한 값에 문제가 있다. 식 (3)에 의거 $Li(x)=\frac{x}{\ln x}\sum_{t=0}^{\infty}\left(\frac{t!}{(\ln x)^t}\right)=\frac{x}{\ln x}\left(1+\frac{1!}{(\ln x)^1}+\frac{2!}{(\ln x)^2}+\frac{3!}{(\ln x)^3}+\cdots\right)$이다.

$x=10$인 경우 $\pi(x)=4$이다. 이 경우 $\frac{x}{\ln x}=4.3429$, $\frac{x}{\ln x}\left(1+\frac{1!}{\ln x}\right)=6.2291$, $\frac{x}{\ln x}\sum_{t=0}^{2}\frac{t!}{(\ln x)^t}=7.8673$, $\frac{x}{\ln x}\sum_{t=0}^{3}$

$\frac{t!}{(\ln x)^t} = 10.0018,$, $\frac{x}{\ln x}\sum_{t=0}^{4}\frac{t!}{(\ln x)^t} = 13.7097$로 발산하며, $t=3$일 때 $\pi(x)$는 x값을 초과한다. $x=100$에 대해서도 동일한 결과가 발생한다. 결국, $Li(x) \sim \frac{x}{\ln x}\sum_{t=0}^{\infty}\frac{t!}{(\ln x)^t}$가 성립하지 않아 $Li(x)$를 소수계량함수로 사용할 수 없다.

표 1. $\pi(x), \frac{x}{\ln x} - \pi(x), Li(x) - \pi(x), R(x) - \pi(x)$

Table 1. $\pi(x), \frac{x}{\ln x} - \pi(x), Li(x) - \pi(x), R(x) - \pi(x)$

x (10^k)	$\pi(x)$	오차		
		$\lfloor \frac{x}{\ln x} \rfloor$	$Li(x)$	$R(x)$
10^1	4	0	2	−1
10^2	25	−3	5	−1
10^3	168	−23	10	0
10^4	1,229	−143	17	−2
10^5	9,592	−906	38	5
10^6	78,498	−6,116	130	−29
10^7	664,579	−44,158	339	−88
10^8	5,761,455	−332,774	754	−97
10^9	50,847,534	−2,592,592	1,701	79
10^{10}	455,052,511	−20,758,029	3,104	1,828
10^{11}	4,118,054,813	−169,923,159	11,588	2,318
10^{12}	37,607,912,018	−1,416,705,193	38,263	1,476
10^{13}	346,065,536,839	−11,992,858,452	108,971	5,773
10^{14}	3,204,941,750,802	−102,838,308,636	314,890	19,200
10^{15}	29,844,570,422,669	−891,604,962,452	1,052,619	−73,218
10^{16}	279,238,341,033,925	−7,804,289,844,393	3,214,632	−327,052
10^{17}	2,623,557,157,654,233	−68,883,734,693,281	7,956,589	598,255
10^{18}	24,739,954,287,740,860	−612,483,070,893,536	21,949,555	3,501,366
10^{19}	234,057,667,276,344,607	−5,481,624,169,369,960	99,877,775	−23,884,333
10^{20}	2,220,819,602,560,918,840	−49,347,193,044,659,701	222,744,644	4,891,825
10^{21}	21,127,269,486,018,731,928	−446,579,871,578,168,707	597,394,254	86,432,204
10^{22}	201,467,286,689,315,906,290	−4,060,704,006,019,620,994	1,932,355,208	127,132,665
10^{23}	1,925,320,391,606,803,968,923	−37,083,513,766,578,631,309	7,250,186,216	

"리만의 소수 계량함수 이외에 $\pi(x)$를 보다 정확히 표현할 수 있는 함수는 존재하는가?" 이 함수를 찾는 것이 본 연구의 핵심이다.

III. 유한급수 $Li(x)$로 $\pi(x)$ 표현

본 장에서 제안하는 공식은 $\frac{x}{\ln x} < \pi(x) < Li(x)$의 특징에 기반하고 있다. 무한급수 $Li(x) \sim \frac{x}{\ln x}\sum_{t=0}^{\infty}\frac{t!}{(\ln x)^t}$는 잘못 계산되었음을 2장에서 증명하였다. 따라서 근사적 무한급수를 유한급수로 한정시킨 함수를 제안한다. 함수를 제안하기 위해 먼저, 식 (4)와 식 (5)를 고찰해 본다.

$$Li_1(x) = \frac{x}{\ln x}\left(\sum_{t=0}^{k}\frac{t!}{(\ln x)^t}\right) \quad (4)$$

$$Li_2(x) = \frac{x}{\ln x}\left(\sum_{t=0}^{\lfloor 0.5k+1 \rfloor}\frac{t!}{(\ln x)^t} - \sum_{t=\lfloor 0.5k \rfloor + 2}^{2k}\frac{t!}{(\ln x)^t}\right) \quad (5)$$

$Li_1(x), Li_2(x)$와 $\pi(x)$의 오차를 비교한 결과는 표 2에 제시되어 있다. 편의상 일반 프로그램으로 표현할 수 있는 계산 정확도로 수행할 수 있는 10^{16}까지 제시하였다.

표 2에서 $0 \le t \le 2k$인 $Li(x) = \frac{x}{\ln x}\left(\sum_{t=0}^{2t}\frac{t!}{(\ln x)^t}\right)$의 유한급수로 $\pi(x)$를 충분히 표현할 수 있음을 알 수 있다. 왜냐하면 $Li_1(x)$은 $10^1 \le x \le 10^{12}$에 대해서는 $Li(x) - \pi(x)$에 비해 오차가 보다 적은 반면 $10^{13} \le x$에서만 오차가 보다 커지는 특징을 갖기 때문이다. 또한, $Li_2(x)$는 $10^{16} \le x$에서만 $Li(x)$보다 오차가 크기 때문이다.

표 2. $Li(x), Li_1(x), Li_2(x)$와 $\pi(x)$의 오차
Table 2. The error of $Li(x), Li_1(x), Li_2(x)$ and $\pi(x)$

x	$\ln x$	$Li_i(x) - \pi(x)$		
		$Li(x)$	$Li_1(x)$	$Li_2(x)$
10^1	2.302585	2	0	0
10^2	4.605170	5	1	0
10^3	6.907755	10	3	-3
10^4	9.210340	17	8	-1
10^5	11.512925	38	25	-11
10^6	13.815511	130	111	59
10^7	16.118096	339	313	100
10^8	18.420681	754	716	403
10^9	20.723266	1,701	1,645	303
10^{10}	23.025851	3,104	3,021	1,048
10^{11}	25.328436	11,588	11,470	1,270
10^{12}	27.631021	38,263	38,245	20,199
10^{13}	29.933606	108,971	110,584	29,220
10^{14}	32.236191	314,890	344,571	164,095
10^{15}	34.538776	1,052,619	1,402,620	973,643
10^{16}	36.841361	3,214,632	7,019,141	4,262,664

본 장에서는 첫 번째로, $\pi(x)$를 정확히 표현하는 공식으로 식 (6)을 제안한다.

$$Li_3(x) = \left\lfloor \frac{x}{\ln x}\left(\sum_{t=0}^{\alpha}\frac{t!}{(\ln x)^t} \pm \beta\right\rfloor \tag{6}$$

여기서 α는 $t = 0, 1, 2, \cdots$를 증가시키면서 $Li(x) \simeq \pi(x)$가 되는 값으로 결정하고 오차 보정 항 β를 구하였다. $Li_3(x)$는 표 3에 제시되어 있다. 결론적으로, $\frac{x}{\ln x}\left(\sum_{t=0}^{\alpha}\frac{t!}{(\ln x)^t} \pm \beta\right)$의 유한급수로 $\pi(x)$를 정확하게 표현할 수 있음을 알 수 있다. 표 3에서는 $[10^{17}, 10^{23}]$의 $Li_3(x)$ 함수는 프로그램의 표현 정확도로 인해 오차가 발생할 수 있기 때문에 변경될 수 있음을 참고하기 바란다. 본 데이터 처리는 Python Ver. 3.1로 처리되었다.

추가로 $x \neq 10^k$가 아닌 경우도 고찰하였다. 예로, $\pi(500)$ 95에 대해 $Li_3(10^3) = \left\lfloor \frac{x}{\ln x}\left(1 + \frac{1!}{(\ln x)^1} + \frac{3!}{(\ln x)^3}\right) \right\rfloor$을 적용한 결과 95를 얻어 $Li_4(500) - \pi(500) = 0$으로 정확한 해를 얻었다.

두 번째로, 식 (7)을 제안한다. 식 (7)은 표 4에 제시되어 있으며, 10^{21}까지 계산되었다. 10^{22}와 10^{23}은 오차로 인해 계산이 정확하게 수행되지 않아 표현하지 않았다.

$$Li_4(x) = \left\lfloor \frac{x}{\ln x}\left(1 + \alpha\frac{k!}{(\ln x)^k} \pm \beta\right) \right\rfloor, k \geq 2 \tag{7}$$

먼저, $Li_3(x)$와 $Li_4(x)$제안하였지만 10^k에 대한 $\pi(x)$를 표현할 수 있는 특징을 찾지 못하여 하나의 정확한 공식은 제안하지를 못하였다. 따라서 추가적으로 식 (8)을 제안한다.

$$\pi(x) = \sqrt{\alpha x} \pm \beta \tag{8}$$

식 (8)로 추정한 결과는 표 5에 제시되어 있다. 여기서 $0 \leq \pi(x) - \sqrt{\alpha x} \leq 8$, $\pi(x) - \sqrt{\alpha x} \pm \beta = 0$의 범위를 갖는특징을 갖고 있다. 또한, α 값에 대해 $k = 1$인 경우 $l(\alpha) = l(k)$, $2 \leq k \leq 4$인 경우 $l(\alpha) = l(k-1)$, $5 \leq k \leq 14$인 경우 $l(\alpha) = l(k-2)$와 $15 \leq k \leq 23$인 경우 $l(\alpha) = l(k-3)$의 규칙을 갖고 있다.

Ⅳ. 결론 및 향후 연구과제

소수정리는 아직까지 정확한 공식을 제시하지 못하고 근사치만을 구할 수 있었다. 또한, 리만의 제타함수가 증명되지 않고 있으며, 제타함수를 이용하여 $R(x)$를 구한 결과도 근사값이다.

본 논문은 유한급수 $Li_3(x) = \left\lfloor \frac{x}{\ln x}\left(\sum_{t=0}^{\alpha}\frac{t!}{(\ln x)^t} \pm \beta\right\rfloor$, $Li_4(x) = \left\lfloor \frac{x}{\ln x}\left(1 + \alpha\frac{k!}{(\ln x)^k} \pm \beta\right) \right\rfloor$로 $x = 10^k$인 $\pi(x)$를 정확히 표현할 수 있음을 보였다. 그러나 k의 값에 따라 α와 β가 모두 달라 일반화된 하나의 공식으로 제시하지는 못하였다. 따라서 비록 추정값을 제시하지만 $\pi(x)$에 대한 하나의 공식으로 $\sqrt{\alpha x} \pm \beta$를 제안하였으며, 이 공식은 리만의 제타함수로 추정한 값보다 좋은 성능을 보였다.

본 논문에 제시된 각각의 10^k의 유한급수 $Li_3(x)$과 $Li_4(x)$에 대해 다른 수식을 제안할 수도 있으며, 하나의 공통된 수식을 유도할 수도 있을 것이다. 이와 관련된 연구는 추후 과제로 남겨둔다.

비록 리만가설이 증명되더라도 소수 분포 패턴으로 소인수를 찾을 수 있는지는 의문이다. 예로, $RSA-100(10^{100})$의 경우, $l(p) = l(q) = l(n)/2$이므로 p, q는 동일한 10^{50}범위에서 임의로 선택된 소수들이다. 따라서 $\pi(10^{50}) - \pi(10^{49})$의 소수들 중 $p < \sqrt{n}$ 모두를 대상으로 소인수분해를 하여야만 한다. 이를 소수의 분포 패턴으로 풀 수 있는지는 의문이다.

추후에는, $\sqrt{\alpha x}\pm\beta$에서 α 값을 결정하는 방법과 주어진 합성수 (공개키) n을 2개의 소수 p,q로 쉽게 소인수분해하는 방법이 존재하는지 여부를 연구할 예정이다.

표 3. $Li_3(x)$
Table 3. $Li_3(x)$

$x=10^k$	$Li_3(x)$	$\pi(x)-Li_3(x)$
10^1	$\left\lfloor \frac{x}{\ln x}(1) \right\rfloor$	0
10^2	$\left\lfloor \frac{x}{\ln x}(\sum_{t=0}^{1}\frac{t!}{(\ln x)^t}-\frac{3!}{(\ln x)^3}) \right\rfloor$	0
10^3	$\left\lfloor \frac{x}{\ln x}(\sum_{t=0}^{1}\frac{t!}{(\ln x)^t}+\frac{3!}{(\ln x)^3}) \right\rfloor$	0
10^4	$\left\lfloor \frac{x}{\ln x}(\sum_{t=0}^{2}\frac{t!}{(\ln x)^t}) \right\rfloor$	0
10^5	$\left\lfloor \frac{x}{\ln x}(\sum_{t=0}^{3}\frac{t!}{(\ln x)^t}-(\frac{4!}{(\ln x)^4}+\frac{10!}{(\ln x)^{10}})) \right\rfloor$ or $\left\lfloor \frac{x}{\ln x}(\sum_{t=0}^{2}\frac{t!}{(\ln x)^t}+\sum_{t=4}^{7}\frac{t!}{(\ln x)^t}) \right\rfloor$	0
10^6	$\left\lfloor \frac{x}{\ln x}(\sum_{t=0}^{3}\frac{t!}{(\ln x)^t}-(\frac{4!}{(\ln x)^4}+\frac{10!}{(\ln x)^{10}})) \right\rfloor$	0
10^7	$\left\lfloor \frac{x}{\ln x}(\sum_{t=0}^{3}\frac{t!}{(\ln x)^t}+\frac{12!}{(\ln x)^{12}}) \right\rfloor$	0
10^8	$\left\lfloor \frac{x}{\ln x}(\sum_{t=0}^{4}\frac{t!}{(\ln x)^t}-(\frac{5!}{(\ln x)^5}-\frac{7!}{(\ln x)^7}+\frac{12!}{(\ln x)^{12}})) \right\rfloor$	0
10^9	$\left\lfloor \frac{x}{\ln x}((\sum_{t=0}^{4}\frac{t!}{(\ln x)^t}+\frac{6!}{(\ln x)^6}+\sum_{t=8}^{9}\frac{t!}{(\ln x)^t})-\frac{11!}{(\ln x)^{11}}) \right\rfloor$	0
10^{10}	$\left\lfloor \frac{x}{\ln x}(\sum_{t=0}^{5}\frac{t!}{(\ln x)^t}+(\frac{11!}{(\ln x)^{11}}+\frac{13!}{(\ln x)^{13}})) \right\rfloor$	0
10^{11}	$\left\lfloor \frac{x}{\ln x}((\sum_{t=0}^{5}\frac{t!}{(\ln x)^t}+\sum_{t=7}^{8}\frac{t!}{(\ln x)^t})-\sum_{t=10}^{14}\frac{t!}{(\ln x)^t}) \right\rfloor$	0
10^{12}	$\left\lfloor \frac{x}{\ln x}(\sum_{t=0}^{6}\frac{t!}{(\ln x)^t}-(\frac{7!}{(\ln x)^7}+\sum_{t=9}^{12}\frac{t!}{(\ln x)^t}-\frac{14!}{(\ln x)^{14}}+\frac{19!}{(\ln x)^{19}})) \right\rfloor$	0
10^{13}	$\left\lfloor \frac{x}{\ln x}(\sum_{t=0}^{6}\frac{t!}{(\ln x)^t}-(\frac{10!}{(\ln x)^{10}}+\sum_{t=12}^{16}\frac{t!}{(\ln x)^t}-\frac{20!}{(\ln x)^{20}})) \right\rfloor$	0
10^{14}	$\left\lfloor \frac{x}{\ln x}((\sum_{t=0}^{6}\frac{t!}{(\ln x)^t}+\sum_{t=8}^{9}\frac{t!}{(\ln x)^t}+\frac{8!}{(\ln x)^8})-(\frac{10!}{(\ln x)^{10}}-\frac{11!}{(\ln x)^{11}}+\sum_{t=14}^{16}\frac{t!}{(\ln x)^t}-\frac{23!}{(\ln x)^{23}})) \right\rfloor$	0
10^{15}	$\left\lfloor \frac{x}{\ln x}(\sum_{t=0}^{7}\frac{t!}{(\ln x)^t}-(\frac{8!}{(\ln x)^8}+\frac{10!}{(\ln x)^{10}}-\sum_{t=12}^{14}\frac{t!}{(\ln x)^t}+\frac{16!}{(\ln x)^{16}}+\frac{20!}{(\ln x)^{20}})) \right\rfloor$	0
10^{16}	$\left\lfloor \frac{x}{\ln x}(\sum_{t=0}^{7}\frac{t!}{(\ln x)^t}-(\frac{8!}{(\ln x)^8}-\frac{9!}{(\ln x)^9}+\sum_{t=10}^{11}\frac{t!}{(\ln x)^t}-\frac{12!}{(\ln x)^{12}}+\frac{13!}{(\ln x)^{13}}-\frac{14!}{(\ln x)^{14}}+\sum_{t=16}^{17}\frac{t!}{(\ln x)^t} -\frac{20!}{(\ln x)^{20}}+\frac{23!}{(\ln x)^{23}})) \right\rfloor$	0
10^{17}	$\left\lfloor \frac{x}{\ln x}((\sum_{t=0}^{10}\frac{t!}{(\ln x)^t}+5\frac{9!}{(\ln x)^9})-(2\sum_{t=13}^{14}\frac{t!}{(\ln x)^t}+\frac{13!}{(\ln x)^{13}}+\frac{21!}{(\ln x)^{21}}+\frac{23!}{(\ln x)^{23}}+\frac{31!}{(\ln x)^{31}})) \right\rfloor$	0
10^{18}	$\left\lfloor \frac{x}{\ln x}((\sum_{t=0}^{8}\frac{t!}{(\ln x)^t}+2\frac{8!}{(\ln x)^8})-(2\frac{10!}{(\ln x)^{10}}+\frac{11!}{(\ln x)^{11}}+\sum_{t=14}^{15}\frac{t!}{(\ln x)^t}-\frac{16!}{(\ln x)^{16}}+\frac{19!}{(\ln x)^{19}}+\frac{21!}{(\ln x)^{21}}-\frac{26!}{(\ln x)^{26}})) \right\rfloor$	0
10^{19}	$\left\lfloor \frac{x}{\ln x}(\sum_{t=0}^{9}\frac{t!}{(\ln x)^t}-(\sum_{t=10}^{11}\frac{t!}{(\ln x)^t}-2\frac{13!}{(\ln x)^{13}}+\sum_{t=15}^{16}\frac{t!}{(\ln x)^t}-\frac{18!}{(\ln x)^{18}}-\frac{23!}{(\ln x)^{23}}-\frac{25!}{(\ln x)^{25}}+\frac{34!}{(\ln x)^{34}})) \right\rfloor$	0
10^{20}	$\left\lfloor \frac{x}{\ln x}((\sum_{t=0}^{9}\frac{t!}{(\ln x)^t}+\frac{12!}{(\ln x)^{12}}+5\frac{13!}{(\ln x)^{13}})-(\frac{14!}{(\ln x)^{14}}-\frac{15!}{(\ln x)^{15}}+\frac{16!}{(\ln x)^{16}}-\frac{17!}{(\ln x)^{17}}+\sum_{t=19}^{21}\frac{t!}{(\ln x)^t}-\frac{26!}{(\ln x)^{26}} -\frac{31!}{(\ln x)^{31}}-\frac{35!}{(\ln x)^{35}})) \right\rfloor$	0
10^{21}	$\left\lfloor \frac{x}{\ln x}(\sum_{t=0}^{9}\frac{t!}{(\ln x)^t}-(\frac{11!}{(\ln x)^{11}}+4\frac{12!}{(\ln x)^{12}}-\sum_{t=14}^{15}\frac{t!}{(\ln x)^t}-3\frac{16!}{(\ln x)^{16}}+\sum_{t=20}^{21}\frac{t!}{(\ln x)^t})) \right\rfloor$	0
10^{22}	$\left\lfloor \frac{x}{\ln x}((\sum_{t=0}^{9}\frac{t!}{(\ln x)^t}+3\frac{10!}{(\ln x)^{10}}+2\frac{11!}{(\ln x)^{11}}+3\frac{12!}{(\ln x)^{12}}+\frac{14!}{(\ln x)^{14}}+\frac{16!}{(\ln x)^{16}})-(\frac{17!}{(\ln x)^{17}}+\frac{18!}{(\ln x)^{18}}-\frac{19!}{(\ln x)^{19}} +\frac{20!}{(\ln x)^{20}}-\frac{21!}{(\ln x)^{21}}+\sum_{t=22}^{23}\frac{t!}{(\ln x)^t}+\frac{30!}{(\ln x)^{30}}+\frac{33!}{(\ln x)^{33}})) \right\rfloor$	0
10^{23}	$\left\lfloor \frac{x}{\ln x}((\sum_{t=0}^{10}\frac{t!}{(\ln x)^t}+6\frac{11!}{(\ln x)^{11}})-(2\frac{12!}{(\ln x)^{12}}-\frac{14!}{(\ln x)^{14}}+\frac{16!}{(\ln x)^{16}}-\frac{20!}{(\ln x)^{20}}+\frac{21!}{(\ln x)^{21}}-\frac{25!}{(\ln x)^{25}}+\frac{28!}{(\ln x)^{28}} +\frac{31!}{(\ln x)^{31}})) \right\rfloor$	0

표 4. $Li_4(x)$
Table 4. $Li_4(x)$

x	α	β	$\pi(x)-Li_4(x)$
10^1	0	0	0
10^2	2	0	0
10^3	9	0	0
10^4	40	$-\frac{6!}{(\ln x)^6}$	0
10^5	176	0	0
10^6	816	0	0
10^7	3,991	$+\frac{11!}{(\ln x)^{11}}$	0
10^8	20,155	$-\frac{13!}{(\ln x)^{13}}$	0
10^9	104,365	$-6\frac{14!}{(\ln x)^{14}}$	0
10^{10}	551,818	$-5\frac{16!}{(\ln x)^{16}}$	0
10^{11}	2,967,545	$+5\frac{18!}{(\ln x)^{18}}$	0
10^{12}	16,184,624	$-9\frac{17!}{(\ln x)^{17}}$	0
10^{13}	89,303,574	$-15\frac{20!}{(\ln x)^{20}}$	0
10^{14}	497,625,074	$-\frac{20!}{(\ln x)^{20}}$	0
10^{15}	2,796,300,171	$-\frac{22!}{(\ln x)^{22}}$	0
10^{16}	15,827,776,599	$-100\frac{26!}{(\ln x)^{26}}$	0
10^{17}	90,159,481,981	$-25\frac{27!}{(\ln x)^{27}}$	0
10^{18}	51,640,795,574	$-34\frac{25!}{(\ln x)^{25}}$	0
10^{19}	2,973,037,792,653	$-215\frac{30!}{(\ln x)^{30}}$	0
10^{20}	17,190,844,388,314	$+122\frac{29!}{(\ln x)^{29}}$	0
10^{21}	99,798,695,987,215	$+32\frac{34!}{(\ln x)^{34}}$	0

표 5. $\sqrt{ax}\pm\beta$
Table 5. $\sqrt{ax}\pm\beta$

x	$\sqrt{\alpha x}\pm\beta$		$\pi(x)-\sqrt{\alpha x}\pm\beta$	
	α	β	$\lfloor\sqrt{\alpha x}\pm\beta\rfloor$	$\lceil\sqrt{\alpha x}\pm\beta\rceil$
10^1	$1^2<2<2^2$	0	0	-1
10^2	$2^2<6<3^2$	0	1	0
10^3	$5^2<28<6^2$	0	1	0
10^4	$12^2<151<13^2$	0	1	0
10^5	$30^2<920<31^2$	0	1	0
10^6	$78^2<6,162<79^2$	0	0	-1
10^7	$210^2<44,166<211^2$	0	4	3
		$+\sqrt{20}$	0	-1
10^8	$576^2<331,944<577^2$	0	-3	-4
		$-\sqrt{10}$	1	0
10^9	$1607^2<2,585,472<1608^2$	0	-2	-3
		$-\sqrt{10}$	1	0
10^{10}	$4550^2<20,707,279<4551^2$	0	-2	-3
		$-\sqrt{10}$	1	0
10^{11}	$13022^2<169,583,754<13023^2$	0	6	5
		$+\sqrt{20}$	1	0
10^{12}	$37607^2<1,414,355,046<37608^2$	0	5	4
		$+\sqrt{20}$	1	0
10^{13}	$109435^2<11,976,135,579<109436^2$	0	-3	-4
		$-\sqrt{10}$	0	-1
10^{14}	$320494^2<102,716,516,260<320495^2$	0	6	5
		$+\sqrt{20}$	1	0
10^{15}	$943768^2<890,698,383,714<943769^2$	0	-5	-6
		$-\sqrt{30}$	0	-1
10^{16}	$2792383^2<7,797,405,110,338<2792384^2$	0	-2	-3
		$-\sqrt{10}$	1	0
10^{17}	$8296416^2<68,830,521,594,788<8296417^2$	0	-8	-9
		$-\sqrt{50}$	0	-1
10^{18}	$24739954^2<612,065,338,159,507<24739955^2$	0	8	7
		$+\sqrt{60}$	0	-1
10^{19}	$74015533^2<5,478,299,161,084,404<74015534^2$	0	-6	-7
		$-\sqrt{30}$	0	-1
10^{20}	$222081960^2<49,320,397,071,188,375<222081961^2$	0	4	3
		$+\sqrt{10}$	1	0
10^{21}	$668102923^2<446,361,515,934,858,213<668102924^2$	0	5	4
		$+\sqrt{20}$	0	-1
10^{22}	$2014672866^2<4,058,906,760,595,500,615<2014672867^2$	0	-2	-3
		$-\sqrt{10}$	1	0
10^{23}	$6088397663^2<37,068,586,103,369,769,908<6088397664^2$	0	-4	-5
		$-\sqrt{20}$	0	-1

참고문헌

[1] D. Zagier, Newman's Short Proof of the Prime Number Theorem," American Mathematical Monthly, Vol. 104, No. 8, pp. 705-708, 1997.

[2] A. O. L. Atkin and D. J. Bernstein,"Prime Sieves Using Binary Quadratic Forms," Mathematics of Computation, Vol. 73, pp: 1023 - 1030, 2004.

[3] B. Riemann, "Ueber die Anzahl der Primzahlen unter einer gegebenen Grösse," Monatsberichte der Königlich Preußischen Akademie der Wissenschaften zu Berlin, 1859. (D. R. Wilkins, "On the Number of Primes Less Than a Given Quantity, 1998.

[4] J. M. Borwein, D. M. Bradley, and R. E. Crandall, "Computational Strategies for the Riemann Zata Function," Journal of Computational Applied Mathematics, Vol. 121, pp: 247-296, 2000.

[5] T. Kotnik, "The Prime-counting Function and its Analytic Approximations," Advanced Computational Mathematics, Vol. 29, No. 1, pp: 55-70, 2008.

[6] D. Goldfeld, "The Elementary Proof of the Prime Number Theorem: An Historical Perspective," The Mathematical Intelligencer, Vol. 31, No. 3, pp. 18-23, 2009.

[7] N. M. Temme, "Exponential, Logarithmic, Sine, and Cosign Integrals," NIST Handbook of Mathematical Functions, Cambridge University Press, 2010.

[8] G. H. Hardy and E. M. Wright, "An Introduction to the Theory of Numbers," 5th ed., pp: 355-356, Oxford, England: Oxford University Press, 1979.

저 자 소 개

이 상 운 (Sang-Un, Lee)

1983년~1987년 : 한국항공대학교 항공전자공학과 (학사)

1995년 ~ 1997년 : 경상대학교 컴퓨터과학과 (석사)

1998년 ~ 2001년 : 경상대학교 컴퓨터과학과 (박사)

2003년 : 강원도립대학 컴퓨터응용과 전임강사

2004년 ~ 2007.2 : 국립 원주대학 여성교양과 조교수

2007.3 ~ 현재 : 강릉원주대학교 과학기술대학 멀티미디어공학과 부교수

관심분야 : 소프트웨어 프로젝트 관리, 소프트웨어 개발 방법론, 소프트웨어 척도, 분석과 설계 방법론, 소프트웨어 시험 및 품질보증, 소프트웨어 신뢰성, 신경망, 뉴로-퍼지, 그래프 알고리즘

e-mail : sulee@gwnu.ac.kr

최 명 복 (Myeong-Bok, Choi)

1992년 : 호서대학교 전자계산학과 (학사)

1994년 : 아주대학교 컴퓨터공학과 (석사)

2001년 : 아주대학교 컴퓨터공학과 (박사)

1997~현재 : 강릉원주대학교 멀티미디어공학과(교수)

2004. 1~현재 : 한국인터넷방송통신학회 이사

관심분야 : 지능형 정보검색, 퍼지응용, 지식표현, 신경망, 지능형 교통제어, 소프트웨어 공학, 알고리즘

e-mail : cmb5859@gmail.com, cmb1@gwnu.ac.kr