最初の五千万の素数*)

D. Zagier
雨宮一郎訳

今日お話しするのは，素数の分布の問題ですが，これは古今の数学者を魅了してきたもので，私も専門外ながら特に関心を持っていました．

素数とは，1より大きい自然数で，1と自分自身以外では割切れないものであることは，よく御存知でしょう．これが数論的な定義ですが，他の定義を与えることも可能です．たとえば，函数論的な定義として，解析函数

$$1-\sin\frac{\pi\Gamma(s)}{s}\Big/\sin\frac{\pi}{s}$$

の整数値の零点，代数的には，

"有限体の標数"，

"Spec $\boldsymbol{Z}$ の点"

または

"非アルキメデス附値"，

組合せ論的には，"漸化式[1]

$$p_{n+1}=\left[1-\log_2\left(\frac{1}{2}+\sum_{r=1}^{n}\sum_{1\leq i_1<\cdots<i_r\leq n}\frac{(-1)^r}{2^{p_{i_1}\cdots p_{i_r}}-1}\right)\right]$$

で与えられるもの"（$[x]$ は x を超えない最大の整数）ということもでき，また，最近論理学者が示したことによれば，変数の0または正の整数値に対する，次の26変数の多項式[2]

$$F(a,b,c,d,e,f,g,h,i,j,k,l,m,n,o,p,q,r,s,t,u,v,w,x,y,z)$$

$$\begin{aligned}
=[k+2][&1-(wz+h+j-q)^2-(2n+p+q+z-e)^2-\\
&(a^2y^2-y^2+1-x^2)^2-(\{e^4+2e^3\}\{a+1\}^2+1-o^2)^2-\\
&(16\{k+1\}^3\{k+2\}\{n+1\}^2+1-f^2)^2-\\
&(\{(a+u^4-u^2a)^2-1\}\{n+4dy\}^2+1-\{x+cu\}^2)^2-\\
&(ai+k+1-l-i)^2-\\
&(\{gk+2g+k+1\}\{h+j\}+h-z)^2-\\
&(16r^2y^4\{a^2-1\}+1-u^2)^2-\\
&(p-m+1\{a-n-1\}+b\{2an+2a-n^2-2n-2\})^2-\\
&(z-pm+pla-p^2l+t\{2ap-p^2-1\})^2-\\
&(q-x+y\{a-p-1\}+s\{2ap+2a-p^2-2p-2\})^2-\\
&(a^2l^2-l^2+1-m^2)^2-(n+l+v-y)^2].
\end{aligned}$$

のとる正値の全体といっても素数の定義になります．しかしここでは，最初の定義だけで充分でしょう．

素数の分布について，皆さんが今後心に刻みつけておいてほしいと思うことが二つあります．一つは，素数が，定義は簡単で，自然数を構成する素材の役割を持っていながら，数学者の研究対象の中で何よりも勝手気ままで手に負えないものだということです．それは，自然数の中に雑草のように生え出で，その生え方は無規則，偶然的で，次にどこに生え出るかは誰にも予測できませんし，与えられた数が素数かどうかの判定もむづかしいのです．もう一つは，前と正反対のことなので，なお当惑するようなことですが，素数の分布が非常な規則性を示すこと，ある法則に終始几帳面に従っているということです．

この二つのうち，第一の主張を実例で見るために，まづ100までの素数と合成数の表を示しましょう．ただし2の他は奇数だけを書きました．

Die ersten 50 Millionen Primzahlen
D. Zagier
Beihefte zur Zeitschrift 《Elemente der Mathematik》
Suppléments à la 《Revue de mathématiques élémentaires》
Beiheft Nr. 15-© Birkhäuser Verlag Basel, 1977
Japanese language serial rights arranged with
Birkhaeuser Verlag AG. Basel, Switzerland
through Tuttle-Mori Agency Inc.. Tokyo

*）本稿は1975年5月5日ボン大学で行なわれた著者の就任講演であり，《Beihefte zu Elemente der Mathematik》(Birkhäuser) no. 15 に掲載された．なお，本記事の存在は山口大学の加藤宗雄氏から教えていただいた．［訳者］

素数	2	3	5	7	11	13	17	19	23	29	31	37	41
	43	47	53	59	61	67	71	73	79	83	89	97	
非素数	9	15	21	25	27	33	35	39	45	49	51	55	57
	63	65	69	75	77	81	85	87	91	93	95	99	

また，次の表は 10000000 の前後 100 以内の素数を示したものです．

9999900 から 10000000 までの素数
9999901
9999907
9999929
9999931
9999937
9999943
9999971
9999973
9999991

10000000 から 10000100 までの素数
10000019
10000079

数が素数であるか否かを一目で判定する方法がないということには誰も異存がないと思います．その上，素数の分布を見ていると解明できない創造の秘密を前にしているような気がするのです．数学の専門家さえ，この秘密に通じていないことは，いつも，より大きい素数を熱心に見つけようとしていることで分かります．平方数のような規則正しく分布する数について，今までに知られていないものを求めることに意義があるとは思えませんが，素数の場合は，ただそれだけのことに大変苦労するのです．たとえば，Lucas は 1876 年に $2^{127}-1$ が素数であることを示しましたが，この記録はその後 75 年間，破られなかったのです．これは，この数の大きさが

$$2^{127}-1 = 170141183460469231731687303715884105727$$

であることを見れば，不思議でもないでしょう．電子計算機がでてきてから，1951 年にはじめて，もっと大きな素数が発見されたのです．次の表は，記録更新の様子を示したものですが[3]，現在の記録保持者は，6002 桁の数，$2^{19937}-1$ です．(これを書き下すわけにもゆきません)．これはギネスブックにものっています*1)．

もっと興味のあるのは，素数分布を支配している法則の探求です．100 までの素数の表は前に示しましたが，これをグラフにしたのが，図 1 です．今後いく度もでてきますが，函数 $\pi(x)$ は x を超えない素数の個数を表し，$x=0$ から出発して，各素数 2, 3, 5 等で 1 だけ飛躍するものです．この図でも分かる通り，局部的な振動を別にすれば，かなり規則正しく増大しています．

p	桁数	発見年	発見者
$2^{127}-1$	39	1876	Lucas
$\frac{1}{17}(2^{148}+1)$	44	1951	Ferrier
$114(2^{127}-1)+1$	41	1951	Miller + Wheeler + EDSAC 1
$180(2^{127}-1)^2+1$	79		
$2^{521}-1$	157	1952	Lehmer + Robinson + SWAC
$2^{607}-1$	183		
$2^{1279}-1$	386		
$2^{2203}-1$	664		
$2^{2281}-1$	687		
$2^{3217}-1$	969	1957	Riesel + BESK
$2^{4253}-1$	1281	1961	Hurwitz + Selfridge + IBM 7090
$2^{4423}-1$	1332		
$2^{9689}-1$	2917	1963	Gillies + ILIAC 2
$2^{9941}-1$	2993		
$2^{11213}-1$	3376		
$2^{19937}-1$	6002	1971	Tuckerman + IBM 360

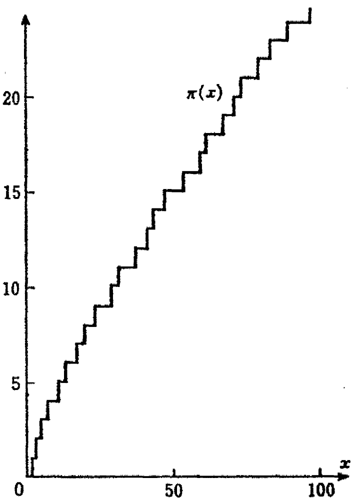

図 1

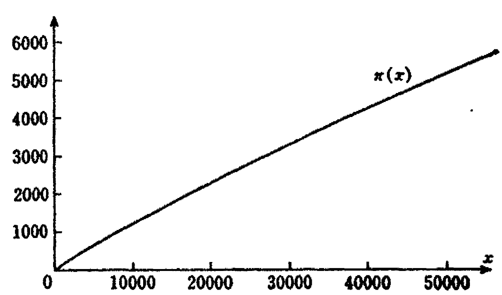

図 2

*1)，*2)，…は訳者注である．

ところが，図2のように，xの範囲を 100 から 50000 まで広げれば，思わずはっとするほどの規則性が現れるのです．このグラフの曲線の上昇のなめらかさは，数学の事実の中で，最も驚嘆すべきものの一つであると思います．

さて，法則性が現れるところには，それを調べようとする人々が集まるものですが，この場合も例外ではありません．まづ，素数の個数の増大の仕方をよく表す実験式を作ることは容易です．100 以下の素数が 25 個で $\frac{1}{4}$ だけあり，1000 以下には 168 個で約 $\frac{1}{6}$，10000 以下には 1229 個で約 $\frac{1}{8}$ あります．これを先へ続けて，素数の割合を計算して見れば，次の表になります．($\pi(x)$ の値が何げなく書いてありますが，これを計算するのに数千時間かかるのです．)

x	$\pi(x)$	$x/\pi(x)$
10	4	2.5
100	25	4.0
1000	168	6.0
10000	1229	8.1
100000	9592	10.4
1000000	78498	12.7
10000000	664579	15.0
100000000	5761455	17.4
1000000000	50847534	19.7
10000000000	455052512	22.0

ここで，x の $\pi(x)$ に対する比が，10 のべきが一つ増すごとに約 2.3 だけ増加しているのが分かりますが，数学者ならすぐにこの 2.3 が 10 の対数 (e を底とする) に近いことに気がつき

$$\pi(x) \sim \frac{x}{\log x}$$

という予想を立てるのです．この記号 ～ は，限りなく増大する x に対して $\pi(x)/(x/\log x)$ が 1 に近づくことを表しています．この予想は，1896 年にはじめて証明されたもので，「素数定理」と呼ばれています．

最大の数学者といわれるガウス (Gauss) は，十五歳のとき，その前年にもらった対数表の中の素数の表をしらべて，これに気がついたのですが，生涯，素数の分布に強い興味を抱いて尨大な計算をしています．Enke[4] への手紙の中で，“ひまな時によく，ところどころ 1000 の間隔の中の素数をしらべて” とうとう三百万 (!) に達し，その分布の様子を，この予想と較べたことを書いています．

素数定理は，$\pi(x)$ が漸近的に，つまり相対誤差の極限 0 で，$x/\log x$ に等しいことを主張しています．しかし，図3で，$\pi(x)$ と $x/\log x$ とのグラフを較べてみますと，$x/\log x$ は定性的には $\pi(x)$ の増加の様子を写し出していますが，その値にはかなりの差があり，細かいところまで近似しているわけではありません．そこで，もっとよい近似がないかと問うのは自然でしょう．x の $\pi(x)$ に対する比の表をもう一度よく見ますと，この比はほとんど $\log x-1$ に等しいことが分かります．ルジャンドル (Legendre)[5] は 1808 年に，もっとくわしいデータについて精密な計算を行った結果，$\log x$ から 1 の代りに，1.08366 を引けば，特によい近似が得られること，すなわち，

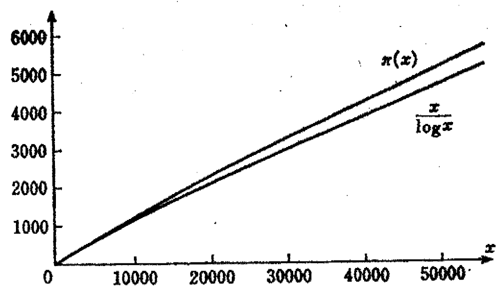

図 3

$$\pi(x) \sim \frac{x}{\log x - 1.08366}$$

となることを発見しました．$\pi(x)$ のもう一つの非常によい近似は，大きな x に対する，x までの素数の頻度は，ほとんど $1/\log x$ に等しいという実験的事実にもとづいて，ガウスによって最初に得られたもので，無限和

$$\mathrm{Ls}(x) = \frac{1}{\log 2} + \frac{1}{\log 3} + \cdots\cdots + \frac{1}{\log x},$$

あるいは，ほとんど同じことですが[6]，積分

$$\mathrm{Li}(x) = \int_2^x \frac{1}{\log t}\,dt$$

によって与えられるものです．$\mathrm{Li}(x)$ と $\pi(x)$ のグラフを較べて見ると，図4程度の精度では，まったく一致してしまうことが分かります．ルジャンドルの近似の方

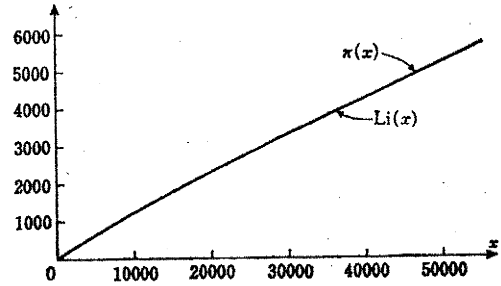

図 4

は，この値域ではもっとよい近似になっていますから書き加える意味がありません．

$\pi(x)$ のもう一つの近似についてのべましょう．リーマン（Riemann）の研究によれば，大きな数 x について，x が素数である確率を考える代りに，素数のべきをも一緒に数え，その場合，素数の平方は半分だけ素数であり，素数の立方は 1/3 だけ素数であるとみなして，その確率を考えれば，もっと $1/\log x$ に近いらしいのです．このことから，

$$\pi(x)+\frac{1}{2}\pi(\sqrt{x})+\frac{1}{3}\pi(\sqrt[3]{x})+\cdots\cdots \simeq \mathrm{Li}(x)$$

という近似が導かれます．これを逆にとけば

$$\pi(x) \simeq \mathrm{Li}(x)-\frac{1}{2}\mathrm{Li}(\sqrt{x})-\frac{1}{3}\mathrm{Li}(\sqrt[3]{x})-\cdots\cdots$$ [7]

となります．この式の右辺の函数はリーマンの名をとって $R(x)$ と書かれます．この函数が $\pi(x)$ を驚くほどよく近似していることは，次の表で示す通りです．

x	$\pi(x)$	$R(x)$
100000000	5761455	5761552
200000000	11078937	11079090
300000000	16252325	16252355
400000000	21336326	21336185
500000000	26355867	26355517
600000000	31324703	31324622
700000000	36252931	36252719
800000000	41146179	41146248
900000000	46009215	46009949
1000000000	50847534	50847455

函数論をある程度知っている人のために，少しつけ加えれば，$R(x)$ は $\log x$ の整函数で，迅速に収束するべき級数

$$R(x)=1+\sum_{n=1}^{\infty}\frac{1}{n\zeta(n+1)}\frac{(\log x)^n}{n!}$$

で表されます．ただし，$\zeta(n+1)$ はリーマンのゼータ函数[8]です．

ここで一つことわっておきたいことがあります．ガウスやルジャンドルによる $\pi(x)$ の近似は実験的に得られたものに過ぎませんが，リーマンの $R(x)$ は理論的に導かれたものです．しかし，そのリーマンも素数定理を証明したわけではありません．それは，1896 年に，Hadamard と，（独立に）de la Vallée Poussin によって始めて証明されたのです．その証明は，リーマンの仕事にもとづいています．

数が素数となる確率について，もう少し計算と実際の結果を示しましょう．前にのべた通り，x 程度の大きさの数が素数である確率は，大体 $1/\log x$ です．そこで，x を含む幅 a の自然数の区間にある素数の個数は，この a が統計上意味を持つほどに大きく，しかも x に較べては充分に小さければ，近似的に $a/\log x$ になるはづです．たとえば，一億から一億十五万までの間には，

$$\frac{150000}{\log(100000000)}=\frac{150000}{18.427\cdots\cdots}\approx 8142$$

ですから，8142 個の素数があると予測できます．

一方，x の近くに任意にとった二つの数が共に素数である確率は，だいたい $1/(\log x)^2$ ですから，x と $x+a$ の間に双子素数の対（11 と 13，59 と 61 のような差が 2 の素数の対）がいくつあるかは，近似的に $a/(\log x)^2$ と考えられるでしょう．n が素数の場合には，$n+2$ が素数となる確率はやや大きいので（たとえば，$n+2$ は必ず奇数です），実際の数は，上の予測より少し大きくなると思われます．ごく簡単な直接的な考察によって[9]，区間 $[x, x+a]$ に入る双子素数の対の個数の期待値は，約 1.3（もっと精密には，1.3203236316）の定数 C によって，$C\cdot a/(\log x)^2$ となります．したがって，一億と一億十五万の間には，約

$$(1.32\cdots\cdots)\frac{150000}{(18.427)^2}\approx 584$$

の双子素数の対があるはづです．ここに Jones と Lal と Blundon[10] が，この区間をはじめ，10 のべきを増した同様の区間の中の，素数と双子素数の対の正確な個数を計算した結果があります．

	素数		双子素数	
間隔	理論	実際	理論	実際
100000000 ～100150000	8142	8154	584	601
1000000000 ～1000150000	7238	7242	461	466
10000000000 ～10000150000	6514	6511	374	389
100000000000 ～100000150000	5922	5974	309	276
1000000000000 ～1000000150000	5429	5433	259	276
10000000000000 ～10000000150000	5011	5065	221	208
100000000000000 ～100000000150000	4653	4643	191	186
1000000000000000 ～1000000000150000	4343	4251	166	161

ごらんの通り，理論と非常によく合っています．これは双子素数については特に驚くべきことです．というのは，その分布がこの予想通りであるかどうかということ

ばかりでなく，そもそも双子素数が無限にあるかどうかということさえ，まだ分かっていないからです．

最後にもう一つ素数の分布に関連したこととして，素数の間隔についてお話ししましょう．素数表を見ると，113 と 127 の間のように，ところどころ，素数のない特に大きな区間があります．x 以下で，素数のない区間の幅の最大値を $g(x)$ としましょう．たとえば，200 以下での最大の幅の区間は，今のべた [113, 127] ですから，$g(200)=14$ です．$g(x)$ はかなり不規則に増大すると思われますが，直接的な議論によって，漸近的な式

$$g(x) \sim (\log x)^2$$

が得られます[11]．次の図を見れば，函数 $g(x)$ はかなりはげしく振動しながらも，$(\log x)^2$ によく合っていることが分かるでしょう．

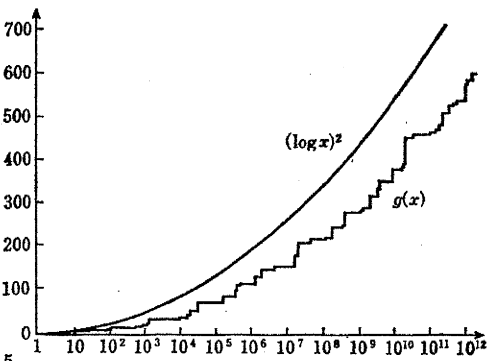

図 5

はじめに素数の分布には規則性と気ままさの両方があるといいましたが，今まで，もっぱら規則性の方について，かなり詳細にしらべてきました．その上，取上げた素数はまだ数千個くらいで，標題に掲げた五千万におよんでいません．ここに $\pi(x)$ のグラフを，ルジャンドル，ガウス，リーマンの近似函数と，一千万[12]までの x について，比較した図があります．前の五万までのグラフ（図 4）で見た通り，この四つの函数は相互に見分けられないほど近いので，ここでは，$\pi(x)$ との差だけを示しました（図 6）．この図が示している事柄は，数論の研究を志す者が避けて通るわけにはゆかないものといえるでしょう．

この図を見ますと，小さな x（大体百万以下）については，ルジャンドルの近似 $x/(\log x-1.08366)$ はガウスの $\mathrm{Li}(x)$ よりかなりよいのですが，五百万以上では $\mathrm{Li}(x)$ の方がよいことが分かります．そして，それ以上の x でも常に $\mathrm{Li}(x)$ の方がよいことが証明できるのです．

一千万までの数の中には素数は六十万くらいしかありませんから，五千万個の素数に達するためには，十億まで行かなければなりません．そこまでの $R(x)-\pi(x)$ のグラフは図 7 のようになります[13]．$R(x)-\pi(x)$ の振動は次第に大きくなりますが，これほど大きな x に対しても，数百程度を超えていないのです．*2)

以上のデータに関連して，$\pi(x)$ の値についてのもう一つの事実をのべましょう．一千万までの図で，ガウスの近似は常に $\pi(x)$ より大きいのですが，このことは，次の図 8 で見られる通り，十億まで同様です．（この図では x の値は対数で取っています．）

たしかにこの図は，x が増大するにつれて，$\mathrm{Li}(x)-\pi(x)$ は確固として無限大に向う印象を与えます．つまり，$\mathrm{Li}(x)$ は常に $\pi(x)$ を過大に評価しているように見えます．（$R(x)$ はいつも $\mathrm{Li}(x)$ より小さいので，これが事実なら，$R(x)$ が $\mathrm{Li}(x)$ よりよい近似を与えるということの確認に資するものといえるでしょう．）しか

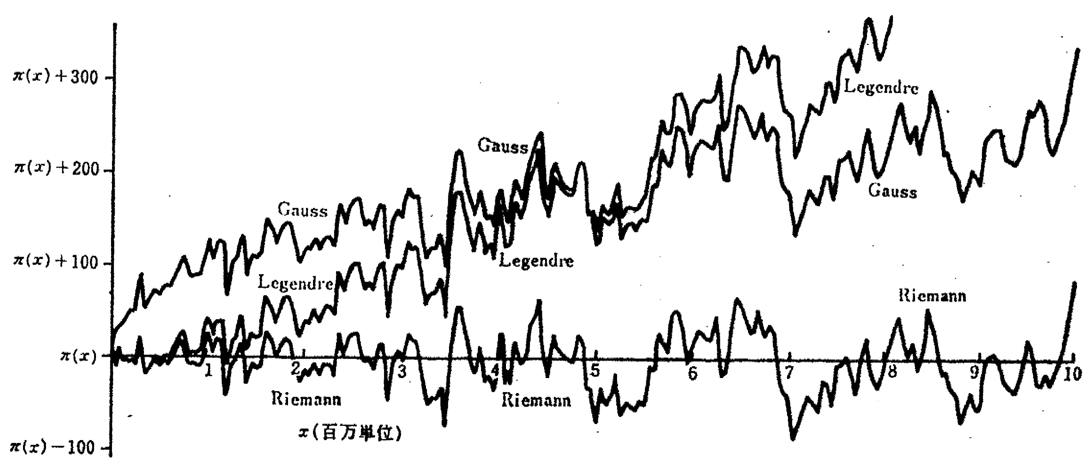

図 6

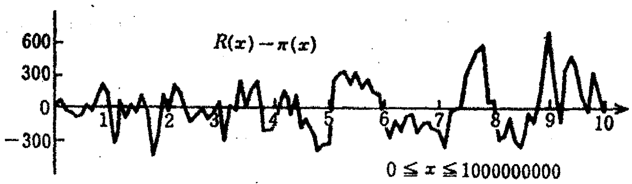

図 7

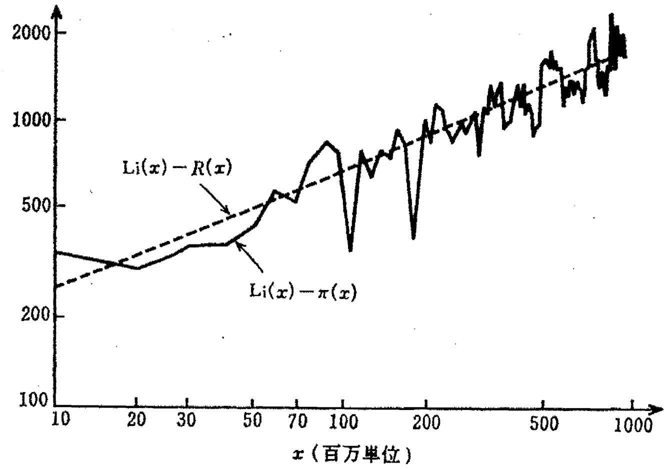

図 8

し，事実はそうではないのです．実際，$\pi(x)$ の振動が非常に大きく，$\mathrm{Li}(x)$ を超えてしまうような x があることが証明できます．今までのところ，そういう x は具体的に分かっていませんし，将来も期待できないでしょう．しかし，Littlewood は，そのような x が存在することを，そしてさらに Skewes[14] は，

$$10^{10^{10^{34}}}$$

以下に在ることを証明したのです．（この数は，数学で何らかの意義を持つ数の中で最大であると，Hardy がいったものです．）とにかくこの例は，素数に関して数値のデータだけにもとづいて結論を出すのは危険であることを示しています．

実験数学のお話しに終らないように，最後に $\pi(x)$ についての理論的な結果を二三のべましょう．数論についてあまり知らない人は，素数であるか否かということは，あまりに偶発的で，それについて何かを証明するなどということは不可能のことと思うかも知れません．ところが，すでに 2200 年前にユークリッドは，素数が無限に在ることを証明しているのです．その論議はほとんど一言でいい表すことができます．すなわち，もし素数が有限個しかなければ，それを全部かけ合せて 1 を加えれば，どの素数でも割切れない数が得られ，それはあり得ないことだというのです．なお，十八世紀にオイラー (Euler) は素数の逆数の和が発散すること，つまりその和が，どんな与えられた数より大きくなり得ることを証明しました．オイラーの証明も非常に簡単で，函数

$$\zeta(s)=1+\frac{1}{2^s}+\frac{1}{3^s}+\frac{1}{4^s}+\cdots\cdots$$

を用いています．この函数の $\pi(x)$ の研究における意義は，その後のリーマンの仕事によって，充分に認識されるようになったのです．このオイラーの結果について注目すべきことは，素数の逆数の和は発散するといっても，今までに知られた素数全部（つまり，五千万個）についての和も 4 より小さいことです[15]．

1850 年にはじめてチェビシェフ (Chebyshev) によって，素数定理の証明への手がかりが得られました．それは，充分に大きな x に対して，

$$0.89\frac{x}{\log x}<\pi(x)<1.11\frac{x}{\log x}$$

ということ，つまり，素数定理は高々 11% の相対誤差で，成立するというのです[16]．チェビシェフの証明は二項定理を用いるもので，非常に見事なものですから，その考えを簡単な形にして（誤差は大きくなりますが）示しましょう．*3)

まず，一方の向きの不等式として，

$$\pi(x)<1.8\frac{x}{\log x}$$

を証明します．これは，$x<1200$ で正しいことが実際

に確かめられます．x が自然数のときに証明すれば充分ですから帰納法によって，これが $n \geqq 600$ で成立すると仮定します．そこで $2n$ に関する中央の二項係数 $\binom{2n}{n}$ に注目します．

$$2^{2n}=(1+1)^{2n}=\binom{2n}{0}+\binom{2n}{1}+\cdots\cdots+\binom{2n}{n}+\cdots\cdots+\binom{2n}{2n}$$

ですから，どの項も 2^{2n} を超えません．一方，

$$\binom{2n}{n}=\frac{(2n)!}{(n!)^2}=\frac{2n\times(2n-1)\times\cdots\cdots\times2\times1}{(n\times(n-1)\times\cdots\cdots\times2\times1)^2}$$

ですから，$2n$ より小さい素数はすべて分子に現れますが，n より大きい素数は分母に現れません．したがって，$\binom{2n}{n}$ は，n と $2n$ の間のどの素数でも割切れ，

$$\prod_{n<p<2n} p \,\Big|\, \binom{2n}{n}$$

となります．この左辺は，$\pi(2n)-\pi(n)$ 個の n より大きい数の積ですから，

$$n^{\pi(2n)-\pi(n)} \leqq \prod_{n<p<2n} p \leqq \binom{2n}{n} < 2^{2n}$$

となり，対数をとれば

$$\pi(2n)-\pi(n) < \frac{2n\log 2}{\log n} < 1.39\frac{n}{\log n}$$

を得ます．仮定によって，

$$\pi(n) < 1.8(n/\log n)$$

ですから，これを加え合せて，

$$\pi(2n) < 3.19\frac{n}{\log n} < 1.8\frac{2n}{\log(2n)} \qquad (n \geqq 600)$$

が得られ，$2n$ についての不等式が成立することが分かります．また，

$$\pi(2n+1) \leqq \pi(2n)+1 < 3.19\frac{n}{\log n}+1$$
$$\leqq 1.8\frac{2n+1}{\log(2n+1)} \qquad (n \geqq 600)$$

ですから，$2n+1$ についても成立し，帰納法が使えるのです．

逆の向きの不等式を得るには，次の簡単な補助定理が必要です．これは，$n!$ を割切る素数のべきについてよく知られた公式を用いて容易に証明することができます[17]．

補助定理． p を素数，p^{ν_p} を，$\binom{n}{k}$ を割切る最大の p のべきとすれば

$$p^{\nu_p} \leqq n$$

系． $\binom{n}{k}=\prod_{p\leqq n} p^{\nu_p} \leqq n^{\pi(n)}$

この不等式を，n に対する二項係数 $\binom{n}{k}$ すべてについて加えれば，

$$2^n=(1+1)^n=\sum_{k=0}^{n}\binom{n}{k} \leqq (n+1)\cdot n^{\pi(n)}$$

となり，対数をとって，

$$\pi(n) > \frac{n\log 2}{\log n}-\frac{\log(n+1)}{\log n} > \frac{2}{3}\frac{n}{\log n} \qquad (n > 200)$$

が得られます．

終りにあたって，リーマンの得た結果について，少しのべましょう．リーマンは素数定理を証明したわけではありませんが，それ以上に驚くべきこと，$\pi(x)$ を正確に表す式を出しているのです．その式は，

$$\pi(x)+\frac{1}{2}\pi(\sqrt{x})+\frac{1}{3}\pi(\sqrt[3]{x})+\cdots\cdots$$
$$=\mathrm{Li}(x)-\sum_{\rho}\mathrm{Li}(x^{\rho})$$

で，右辺の和はゼータ函数 $\zeta(s)$ の零点 ρ すべてにわたるものです[18]．この零点は，（トリヴィアルな零点と呼ばれる $\rho=-2,-4,-6,\cdots$ のこの和に対する影響は，ほとんど無視してよいほどですから，それを除外すれば）みな実数部分が 0 と 1 の間にある複素数で，最初の十個は次に示す通りです[19]．

$$\rho_1=\frac{1}{2}+14.134725\,i, \qquad \bar{\rho}_1=\frac{1}{2}-14.134725\,i,$$

$$\rho_2=\frac{1}{2}+21.022040\,i, \qquad \bar{\rho}_2=\frac{1}{2}-21.022040\,i,$$

$$\rho_3=\frac{1}{2}+25.010856\,i, \qquad \bar{\rho}_3=\frac{1}{2}-25.010856\,i,$$

$$\rho_4=\frac{1}{2}+30.424878\,i, \qquad \bar{\rho}_4=\frac{1}{2}-30.424878\,i,$$

$$\rho_5=\frac{1}{2}+32.935057\,i, \qquad \bar{\rho}_5=\frac{1}{2}-32.935057\,i$$

零点の共役複素数もまた零点になることは容易に分かりますが，その実数部分がみなちょうど $\frac{1}{2}$ であるということはまだ証明されていません．これが有名なリーマン予想で，これを仮定すれば，数論上の非常に進んだ結果が導かれるのです[20]．この予想は，七百万個の零点については正しいことが分かっています．*4)

前にのべたリーマンの函数 $R(x)$ を用いれば，リーマンの与えた式は，

$$\pi(x)=R(x)-\sum_{\rho}R(x^{\rho})$$

の形に書くことができます．この式から，$\pi(x)$ の第 k 番目の近似函数，

$$R_k(x)=R(x)+T_1(x)+T_2(x)+\cdots\cdots+T_k(x)$$

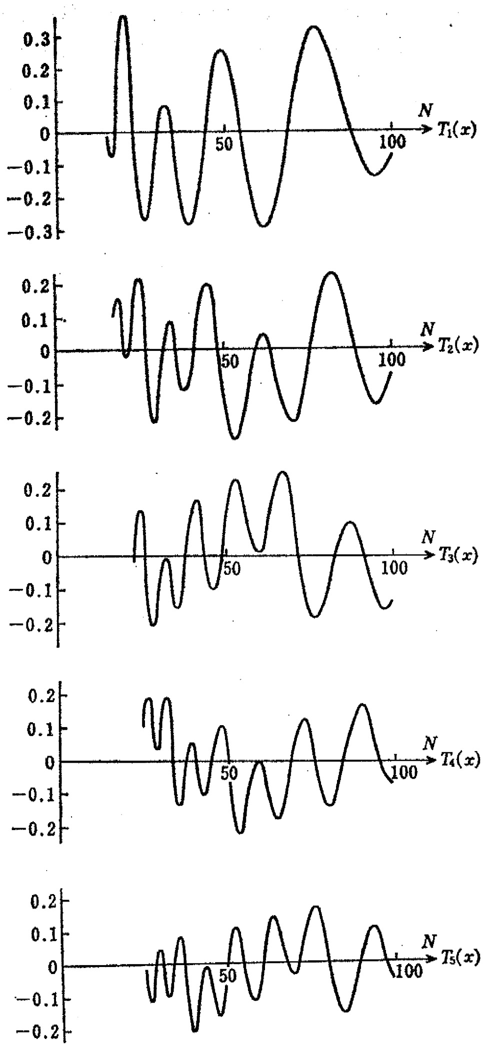

図 9

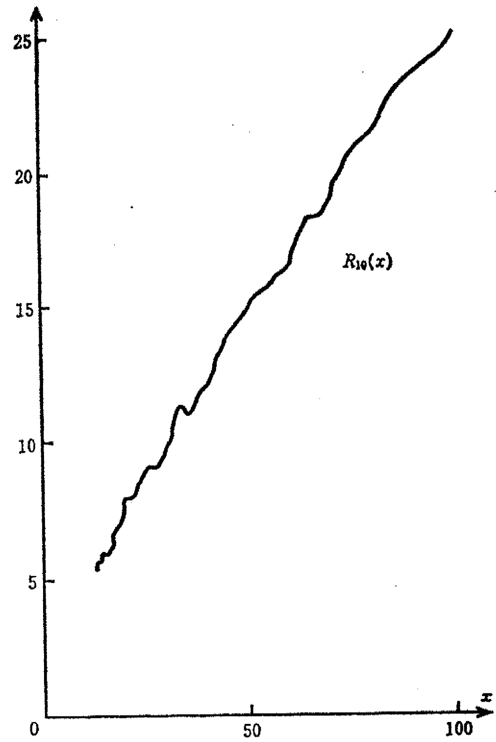

図 10

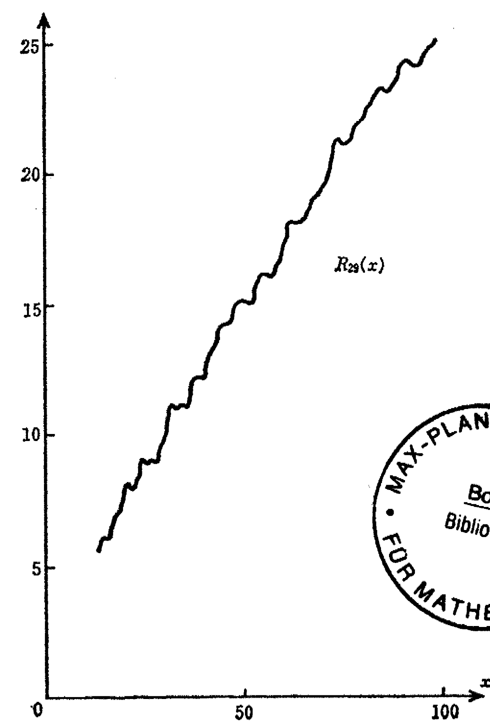

図 11

が得られます．ただし，各 n に対して，$T_n(x) = -R(x^{\rho_n}) - R(x^{\bar{\rho}_n})$ は，ゼータ函数の零点の第 n 番目の共役対に対する項を表すのです．どの $T_n(x)$ もなめらかな振動する函数で，$T_1(x)$ から $T_5(x)$ までのグラフは，図 9 の通りです[21]．$R_k(x)$ も当然なめらかな函数で，k が増大するにつれて，$\pi(x)$ に近づきます．ここに実例として第 10 番目と 29 番目の近似函数のグラフがあります（図 10, 11）．なお，この二つのグラフを，$x = 100$ までの $\pi(x)$ のグラフと較べたのが図 12 です．

これらの図や今までに示した図が，素数の分布の示す絶大な美と驚異について強い印象を皆様に与えたことと信じます．

MAX-PLANCK-INSTITUT FÜR MATHEMATIK
Bonn
Bibliothek

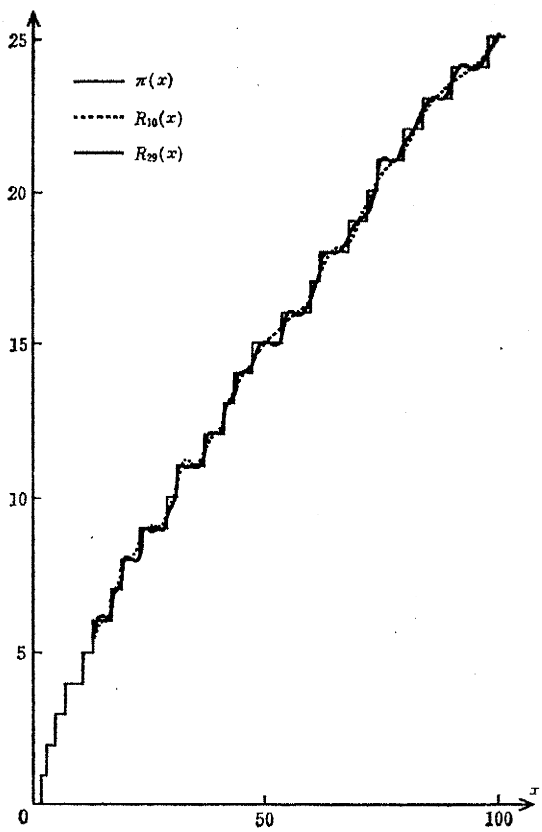

図 12

註

［1］ J. M. Gandhi, Formulae for the n-th prime, Proc. Washington State Univ. Conf. on Number Theory, Washington State Univ., Pullman, Wash., 1971, 96–106

［2］ J. P. Jones, Diophantine representation of the set of prime numbers, Notices of the AMS 22 (1975) A—326.

［3］ この表の素数の多くが $M_k = 2^k-1$ の形をしていることには理由がある．ルカスの定理によれば，$M_k (k \geqq 2)$ が素数であるための必要十分条件は，M_k が L_{k-1} を割切ることで，L_n は帰納的に，$L_1 = 4, L_{n+1} = L_n{}^2-2$ によって定義される（すなわち，$L_2 = 14, L_3 = 194, L_4 = 37634, \cdots$）．したがって，$M_k$ が素数か否かの判定は，同じぐらいの大きさの他の数の場合よりもはるかに容易である．2^k-1 の形の素数（この k も当然素数）はメルセンヌ数と呼ばれ（メルセンヌ (Mersenne) は，1644 年に 10^{79} 以下のこの形の素数のほぼ正確な表をつくったフランスの数学者），まったく別の数論の問題に重要な役割を演ずる．ユークリッドは，2^p-1 が素数ならば，$2^{p-1}(2^p-1)$ は“完全数”（自分自身を除いた約数の和に等しい数）であることを発見した．（たとえば，$6 = 1+2+3$, $28 = 1+2+4+7+14$, $496 = 1+2+4+8+16+31+62+124+248$.）またオイラーは偶数の完全数はこの形のものに限ることを示した．奇数の完全数があるか否かは分かっていない．もしあるとすれば，少なくとも 10^{100} 以上である．なお，$p < 20000$ に対して 2^p-1 が素数になるものはちょうど 24 個ある．

［4］ C. F. Gauss, 全集 II (1872) 444～447. $\pi(x)$ のさまざまな近似の歴史を論じ，ここで引用した手紙の英訳ものせているものとしては，L. J. Goldstein, A history of the prime number theorem, Amer. Math. Monthly, 80 (1973) 599—615.

［5］ A. M. Legendre, Essai sur la theorie de Nombres, 2nd edition, Paris, 1808, p. 394.

［6］ より精確には，

$$\mathrm{Ls}(x)-1.5 < \mathrm{Li}(x) < \mathrm{Ls}(x).$$

つまり，$\mathrm{Li}(x)$ と $\mathrm{Ls}(x)$ の差は有界である．$\mathrm{Li}(x)$ は次のように，コーシーの主値によって定義されるのが普通である．

$$\mathrm{Li}(x) = \int_0^x \frac{dt}{\log t} \overset{\mathrm{DEF}}{=} \lim_{\epsilon \to 0}\left(\int_0^{1-\epsilon} \frac{dt}{\log t} + \int_{1+\epsilon}^x \frac{dt}{\log t}\right)$$

ただし，この定義の $\mathrm{Li}(x)$ は，本文で与えたものと定数だけの差がある．

［7］ 右辺の係数は次のように定められる．$\mathrm{Li}(\sqrt[n]{x})$ の係数は，n が偶数個の異なる素数の積であるとき $+\frac{1}{n}$，奇数個の異なる素数の積であるとき $-\frac{1}{n}$，素数のべきを因子に持つとき 0 とする．

［8］ この函数の別の表現に，

$$R(x) = \int_0^\infty \frac{(\log x)^t dt}{t\Gamma(t+1)\zeta(t+1)}$$

（$\zeta(s)$ はリーマンゼータ函数，$\Gamma(s)$ はガンマ函数）および

$$R(e^{2\pi x}) \doteqdot \frac{2}{\pi}\left(\frac{2}{B_2}x + \frac{4}{3B_4}x^3 + \frac{6}{5B_6}x^5 + \cdots\cdots\right)$$
$$= \frac{2}{\pi}\left(12x + 40x^3 + \frac{252}{5}x^5 + \cdots\cdots\right)$$

がある（B_k は k 番目のベルヌイ数，$\doteqdot$ は両辺の差が，$x \to \infty$ に対して 0 に収束すること）．どちらも Ramanujan による．

G. H. Hardy, Ramanujan: Twelve Lectures on

Subjects Suggested by His Life and Work, Cambridge University Press, 1940, Chap. 2 参照.

[9] 任意にとった二つの数の組 (m, n) に対して，m と n が共に素数 p で割れない確率は明らかに $((p-1)/p)^2$ で，任意にとった数 n に対して，n と $n+2$ が共に p で割れない確率は，$p=2$ ならば $\frac{1}{2}$，$p \neq 2$ ならば $(p-2)/p$ である．したがって，n と $n+2$ が共に p で割れない確率は，二つ独立にとった数が共に p で割れない確率に，$p=2$ のときは 2 を，$p \neq 2$ のときは，$((p-2)/p)(p^2/(p-1)^2)$ を乗じたものになっているので，問題の確率は，

$$C = 2 \cdot \prod_{\substack{p>2 \\ p\text{素数}}} \frac{p^2-2p}{p^2-2p+1} \fallingdotseq 1.32032$$

を乗じてよい．より詳細な議論は，G. H. Hardy, E. M. Wright, An Introduction to the Theory of Numbers, Clarendon Press, Oxford, 1960, §22. 20 (p. 371—373).

[10] M. F. Jones, M. Lal, and W. J. Blundon, Statistics on certain large primes, Math. Comp. 21 (1967) 103—107.

[11] D. Shanks, On maximal gaps between succesive primes, Math. Comp. 18 (1964), 646—651, $g(x)$ のグラフは次の二論文の表による．L. J. Lander and T. R. Parkin, On first appearance of prime differences, Math. Comp. 21 (1967) 483—488, R. P. Brent, The first occurrence of large gaps between successive primes, Math. Comp. 27 (1973) 959—963.

[12] このグラフのデータは Lehmer の素数表からとった．(D. N. Lehmer, List of Prime Numbers from 1 to 10006721, Hafner Publishing Co., New York, 1956).

[13] これと次のグラフは，D. C. Mapes, Fast method for computing the number of primes less than a given limit, Math, Comp. 17 (1963), 179—185 に与えられた $\pi(x)$ の値にもとづく．この値は前のグラフに用いた Lehmer のものと異なり，x までの素数を数えるのではなく，$\pi(x)$ の式から計算されている．

[14] S. Skewes, On difference $\pi(x)-\mathrm{Li}(x)$ (I), J. London Math. Soc, 8 (1933) 277—283. この限界の証明に，Skewes は後述のリーマン予想を仮定しているが，22 年後 (On the difference $\pi(x)-\mathrm{Li}(x)$ (II), Proc. London Math. Soc. (3) 5 (1955), 48—70) その仮定なしに，(はるかに大きな) 限界

$$10^{10^{10^{964}}}$$

以下の x で，$\pi(x) > \mathrm{Li}(x)$ となることを証明している．この限界は，Cohen と Mayhew により，$10^{10^{529.7}}$ に，また Lehman (On the difference $\pi(x)-\mathrm{Li}(x)$, Acta Arithm. 11 (1966), 397—410) によって，1.65×10^{1165} に下げられた．なお，Lehman は，1.53×10^{1165} と 1.65×10^{1165} の間に，少なくとも 10^{500} の幅の区間があり，その中のどの x でも，$\pi(x) > \mathrm{Li}(x)$ となることまで示した．Lehman の研究によれば，6.663×10^{370} 附近に，$\pi(x) > \mathrm{Li}(x)$ となる x があるらしく，また 10^{20} 以下にはこのような x はないらしい．

[15] すなわち，(ガウスによって 1796 年に予想され，Mertens が 1874 年に証明した通り)

$$\sum_{p<x} \frac{1}{p} = \log \log x + C + \varepsilon(x)$$

ただし，$x \to \infty$ に対して $\varepsilon(x) \to 0$ で，$C \approx 0.261497$ は定数．この和は $x = 10^9$ のとき 3.3 より小さく，$x = 10^{18}$ のときさえなお 4 に達しない．

[16] P. L. Chebyshev, Recherches nouvelles sur nombres premiers, Paris 1851, CR Paris 29 (1849), 397—401, 738—739. この証明をドイツ語で現代的にのべたものとしては，W. Schwarz, Einführung in methoden und Ergebnisse der Primzahltheorie BI-Hochschultaschenbuch 278/278a, Mannheim 1969, Chapt. II. 4, p. 42–48.

[17] $n!$ を割る p の最高べきは，$p^{[n/p]+[n/p^2]+\cdots}$ である．ただし $[x]$ は x をこえない最大の整数．ゆえに補助定理の ν_p は，

$$\nu_p = \sum_{r \geqq 1} ([n/p^r] - [k/p^r] - [u-k/p^r])$$

で与えられる．この和の各項は 0 または 1 で，$r > (\log n/\log p)$ に対しては 0 である ($[n/p^r] = 0$ であるから)．したがって，$\nu_p \leqq (\log n/\log p)$ であり，補助定理の結果を得る．

[18] ここで与えた $\zeta(s)$ の $1+\frac{1}{2^s}+\frac{1}{3^s}+\cdots\cdots$ としての定義は，s の実数部分が 1 より大きい複素数のときだけ意味を持つが (その場合だけ級数は収束するので)，この範囲には $\zeta(s)$ の零点はない．しかし函数 $\zeta(s)$ は複素平面全体で定義することができ，そこで零点を考えることができる．$\zeta(s)$ の定義域を $\mathrm{Re}(s) > 0$ まで拡大する簡単な方法は，$\mathrm{Re}(s) > 1$ で成立する等式

$$(1-2^{1-s})\zeta(s) = 1+\frac{1}{2^s}+\frac{1}{3^s}+\cdots\cdots$$

$$-2\left(\frac{1}{2^s}+\frac{1}{4^s}+\frac{1}{6^s}+\cdots\cdots\right)$$
$$=\sum_{n=1}^{\infty}\frac{(-1)^{n-1}}{n^s}$$

を用い，右辺の級数は実数部分が正のすべての複素数で収束することに注目すればよい．この式により，$\zeta(s)$ の"重要な"零点，つまり零点 $\rho=\beta+i\gamma$ で $0<\beta<1$ となるものは，次の二つの方程式で初等的に定められる．

$$\sum_{n=1}^{\infty}\frac{(-1)^{n-1}}{n^\beta}\cos(\gamma\log n)=0,$$

$$\sum_{n=1}^{\infty}\frac{(-1)^{n-1}}{n^\beta}\sin(\gamma\log n)=0.$$

リーマンの公式における零点 ρ についての和は絶対収束しないので，正しい順序 ($\mathrm{Im}(\rho)$ の絶対値の大きさの順に) 加えなければならない．

リーマンは $\pi(x)$ のこの正確な式をすでに 1859 年に出しているが，1895 年に von Mangoldt がはじめて証明した．

[19] これらの零点はすでに 1903 年 Gram が計算している．(J.-P. Gram, Sur les zéros de la fonction $\zeta(s)$ de Riemann, Acta. 27 (1903), 289—304.) リーマンのゼータ函数の非常に見事な解説と，その零点の計算の方法をのべたものとしては，H. M. Edwards, Riemann's Zeta Function, Academic Press, New York, 1974.

[20] リーマン予想からは，(実はそれと同値であるが) $\pi(x)$ に対するガウスの近似 $\mathrm{Li}(x)$ の誤差は $x^{1/2}\cdot\log x$ の定数倍をこえないことが導かれる．現在のところ，この誤差が，ある定数 $C<1$ に対して x^C より小さいということさえ分かっていない．

[21] これと次の三つのグラフは，H. Riesel, G. Göhl, Some Calculations related to Riemann's Prime number formula, Math. Comp. 24 (1970), 969—983. からとった．

訳者註

*1) その後の記録は次の通り．

p	桁数	発見年	発見者
$2^{21701}-1$	6533	1978	C. Noll+L. Nickel+CDC Cyber-174
$2^{23209}-1$	6987	1979	C. Noll+CDC Cyber-174
$2^{44497}-1$	13395	1979	D. Slowinski+H. Nelson+Cray-I
$2^{86243}-1$	25962	1982	D. Slowinski+Cray-I
$2^{132049}-1$	39751	1983	D. Slowinski+Cray-XMP

*2) H. Riesel, Prime Number and Computer Methods for Factorization, Birkhäuser 1985 に次の表がある．

x	$\pi(x)$	$\mathrm{Li}\,x-\pi(x)$	$R(x)-\pi(x)$
10^2	25	5	1
10^3	168	10	0
10^4	1229	17	−2
10^5	9592	38	−5
10^6	78498	130	29
10^7	664579	339	88
10^8	5761455	754	97
10^9	50847534	1701	−79
10^{10}	455052511	3104	+1828
10^{11}	4118054813	11588	−2318
10^{12}	37607912018	38263	−1476
10^{13}	346065536839	108971	−5773
10^{14}	3204941750802	314890	−19200
10^{15}	29844570422669	1052619	73218
10^{16}	279238341033925	3214632	327052

(この表，および *1) の記録について和田秀男氏から御教示をいただいた．)

*3) 以下原文に筋の通らないところがあり，少し訂正した．これについては，[9] で引用した Hardy-Wright の書および内山三郎，素数の分布，宝文館 1970 参照．

*4) この数は 200000001 個におよんでいる．R. P. Brent, J. Van de Lune, H. J. J. Riele, D. T. Winter, The first 200000001 zeros of Riemann's zeta function, Computational methods in number theory, Part II, 389-403 Mathematical Centre Tracts 155, Mathematisch Centrum Amsterdam, 1982.