数理解析研究所講究録
310巻 1977年 93-104

素数と計算機

学習院大 理　田中 穣

素数の分布状態について，古くから数値的な実験が試みられてきたが，近年，電子計算機の出現によって実験の能率が飛躍的に向上した．こういう実験は理論を踏まえて計画を立てなければならない．

§1. $\pi(x)$

§2. $\psi(x)$

§3. 双子素数

§4. 大きい素数

§1. $\pi(x)$. xをこえない素数の個数を$\pi(x)$で表わす．$\pi(x)$の正確な値を求めるには古来のふるい法による．

$\pi(10)=4$, $\pi(100)=25$, $\pi(1000)=168$,

$\pi(10000)=1229$, $\pi(10^5)=9592$, $\pi(10^6)=78498$,

$\pi(10^7)=664579$, $\pi(10^8)=5761455$,

$\pi(10^9)=50847534$, $\pi(10^{10})=455052512$.

Lehmer [6], Mapes [8].

さて$\pi(x)$の理論的な結果といえば，まず素数定理をあげ

なければならない.

素数定理.

$$\pi(x) \sim \frac{x}{\log x} \quad (x \to \infty).$$

しかし, $x/\log x$ よりも

$$P(x) = \sum_{n=1}^{\infty} \frac{(\log x)^n}{n!\, n\zeta(n+1)}, \quad \zeta(n+1) = \sum_{k=1}^{\infty} \frac{1}{k^{n+1}}$$

の方がはるかに良く $\pi(x)$ に近似する.

Mapes [8] によると, $\pi(x) - P(x)$, $x = 10^7(10^7)10^8$ は

$-87, 37, 42, 85, 68, -38, 45, -110, -227, -96$

で, $\pi(x) - P(x)$, $x = 10^8(10^8)10^9$ は

$-96, -152, -29, 142, 351, 82, 213, -68, -733, 80$

である. このわずかな数値からもわかるように, $P(x)$ は $\pi(x)$ に鋭く近接し, しかも $\pi(x)$ と $P(x)$ とが seesaw match を続けている.

では理論的に, $\pi(x) - P(x)$ についてどんなことが判っているのか. まず $P(x) \sim x/\log x$ であるから, 素数定理は $\pi(x) \sim P(x)$ と書いてもよい. また

$$\liminf_{x \to \infty} \frac{\pi(x) - P(x)}{\frac{\sqrt{x}}{\log x} \log\log\log x} < 0, \quad \limsup_{x \to \infty} \frac{\pi(x) - P(x)}{\frac{\sqrt{x}}{\log x} \log\log\log x} > 0$$

であることが証明されている. 従って, $x \to \infty$ のとき, $\pi(x) - P(x)$ は符号の変化を限りなく繰り返す. この傾向が

上記の実験の結果にもよく表われている。この $P(x)$ に初めて気付いたのは Riemann である。Riemann はどんな手がかりで $P(x)$ に気付いたのか、ここでは $P(x)$ を導き出す手順を平易な方法で解説してみよう。もちろん heuristic である。素数定理を証明するのに，初手から $\pi(x)$ を取り扱う代りに

$$\psi(x)=\sum_{n\leqq x}\Lambda(n),$$

$$\Lambda(n)=\begin{cases}\log p & (n\text{が素数べき } p^m \text{ のとき})\\ 0 & (n=1,\ \text{または } n \text{ が2個以上の相異なる素因数をもつとき})\end{cases}$$

とおいて，　$\psi(x)\sim x\quad(x\to\infty)$

を証明しておくと，容易に素数定理へ移行することができる。$\psi(x)$ を経由する方が証明が円滑にゆく。

さて $\psi(x)\sim x$ は

$$\sum_{n\leqq x}\Lambda(n)\sim\sum_{n\leqq x}1$$

であるから

$$\sum_{n\leqq x}\frac{\Lambda(n)}{\log n}\sim\sum_{n\leqq x}\frac{1}{\log n}$$

も成り立つであろう。ところで左辺は $\Lambda(n)$ の定義から

$$\sum_{k=1}^{\infty}\frac{1}{k}\pi\left(x^{\frac{1}{k}}\right)$$

と書くことができる。また右辺と

$$li(x)=\lim_{\delta\to 0}\left(\int_0^{1-\delta}+\int_{1+\delta}^{x}\right)\frac{du}{\log u}$$

との差は僅少である。こうして上記の漸近式は

$$\sum_{k=1}^{\infty}\frac{1}{k}\pi(x^{\frac{1}{k}})\sim li(x)$$

となる。ここへ Möbius の反転公式を使うと

$$\pi(x)\sim\sum_{k=1}^{\infty}\frac{\mu(k)}{k}li(x^{\frac{1}{k}})$$

となるが，右辺を更に変形することができる．

$$li(x)=\gamma+\log\log x+\sum_{n=1}^{\infty}\frac{(\log x)^n}{n!\,n}\quad(\gamma\text{ は Euler 定数}),$$

$$\sum_{k=1}^{\infty}\frac{\mu(k)}{k}=0,\quad \sum_{k=1}^{\infty}\frac{\mu(k)\log k}{k}=-1$$

であるから

$$\sum_{k=1}^{\infty}\frac{\mu(k)}{k}li(x^{\frac{1}{k}})=1+P(x)$$

であることがわかる。 Lehmer [5], Introduction 参照．

§2. $\psi(x)$. 素数定理の証明に限らず，$\pi(x)$ に対して，あることを証明するのに，まず $\psi(x)$ に対して対応する

結果を求めておいて，あとで $\pi(x)$ へ移行するのが得策である．Hardy-Wright [4], p.340 に，$\psi(x)$ は $\pi(x)$ よりも 'natural' な関数であると評している．そんなら，$\psi(x)$ を $\pi(x)$ のための補助手段として使う立場を捨てて，$\psi(x)$ を研究対象と考えても差支えないであろう．むしろ，その方が 'natural' な態度である．田中は $\psi(x)$ の実験を思い立ち，学習院大学計算センター設置 MELCOM 7500 を使って $\psi(x)-x$, $x=10^4(10^4)10^8$ を計算した．数表 I は $\psi(x)-x$, $x=10^6(10^6)10^8$ を抜き書きしたものである．切り上げ切り捨ての影響が集積するのを押えるため倍精度計算を行った．

$\psi(x)$ の理論的な結果としては，$\psi(x)\sim x$ であることはすでに述べたが，

$$\liminf_{x\to\infty}\frac{\psi(x)-x}{\sqrt{x}\log\log\log x}<0,\quad \limsup_{x\to\infty}\frac{\psi(x)-x}{\sqrt{x}\log\log\log x}>0$$

であることが証明されている．従って，$x\to\infty$ のとき，$\psi(x)-x$ は符号の変化を限りなく繰り返すわけである．数表 I の数値にもこの傾向が現われている．

§3．双子素数．$p, p+2$ がともに素数のとき $(p, p+2)$ は双子素数の組であるという．たとえば $(3,5)$, $(5,7)$, $(11,13)$, $(17,19)$, …．双子素数の組が無限にあるのかどう

が未解決である。しかし，xを越えない双子素数の組の個数を $\pi_2(x)$ とすると，

$$\pi_2(x) \sim C\frac{x}{\log^2 x}, \qquad C = 2\prod_{p>2}\left\{1-\frac{1}{(p-1)^2}\right\}$$

であることが予想されている。 $C = 1.32032\cdots$

この予想に関して，Hardy-Littlewood [3], Hardy-Wright [4], Postscript on prime-pairs 参照.

$\pi_2(x)$ の正確な値を挙げてみると

$\pi_2(10^5) = 1224$, $\pi_2(10^6) = 8169$, $\pi_2(10^7) = 58980$,

$\pi_2(10^8) = 440312$, $\pi_2(10^9) = 3424506$,

$\pi_2(10^{10}) = 27412679$. Brent [1] による.

さて双子素数の場合も，$\pi_2(x)$ より

$$\psi_2(x) = \sum_{n \leqq x} \Lambda(n)\Lambda(n+2)$$

の方が 'natural' な関数であろう。田中は MELCOM 7500 を使って $\psi_2(x) - Cx$, $x = 10^4(10^4)10^8$ を計算した。数表IIは $\psi_2(x) - Cx$, $x = 10^6(10^6)10^8$ を抜き書きしたものである。

次の予想はどうであろうか。

$\psi_2(x) \sim Cx$, かつ $\psi_2(x) - Cx$ は $x \to \infty$ のとき，符号の変化を限りなく繰り返す。

数表I，IIを比べると，$\psi_2(x) - Cx$ の方が $\psi(x) - x$ より

符号の変化が緩慢なようである、もっと実験の範囲を拡げなければならない、

§4. 大きい素数、pが素数のとき $M_p = 2^p - 1$ を Mersenne 数という、$p<20000$ に M_p が素数となる p が24個ある、

$$p = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127,$$
$$521, 607, 1279, 2203, 2281, 3217, 4253,$$
$$4423, 9689, 9941, 11213, 19937.$$

M_{127}（39けた）は電子計算機のない時代に人間の知っていた最大の素数で，M_{19937}（6002けた）は現在，人間の知っている最大の素数である、M_{19937} は Tuckerman [13] によって発見された、M_pが素数であるかどうかを判定するのに Lucas の定理がある.

数列$\{s_k\}$を $s_1=4$, $s_{k+1}=s_k^2-2$ によって与えるとき，$M_p\ (p>2)$ が素数であるための必要十分条件は s_{p-1} が M_p で割り切れることである.

M_p が素数のとき $2^{p-1}M_p$ は完全数である、偶数の完全数はこのような数だけである、奇数の完全数があるのかどうか未解決である、しかし，10^{100} より小さい奇数の完全数のないことが確かめられている、奇数が完全数であるための必要

条件がいくつもあって，それらを組み合わせた複雑な case study である．Hagis [2]，Stubblefield [10] 参照．

ところで，ずば抜けて大きい双子素数も見つかっている．

$9\cdot 2^{43}\pm 1$，$9\cdot 2^{63}\pm 1$，$9\cdot 2^{211}\pm 1$，$45\cdot 2^{189}\pm 1$，$75\cdot 2^{43}\pm 1$

$99\cdot 2^{65}\pm 1$，$10\cdot 3^{102}\pm 1$，$68\cdot 3^{30}\pm 1$，$70\cdot 3^{25}\pm 1$，

$76\cdot 3^{139}\pm 1$，$82\cdot 3^{26}\pm 1$，$94\cdot 3^{55}\pm 1$

は双子素数である．$76\cdot 3^{139}\pm 1$ は現今，人間の知っている最大の双子素数であろう．Riesel [9]，Williams-Zarnke [15] による．このような数が素数であることを保証する定理がある．

N の素因数がわかっていると，N+1 が素数であるかどうかの判定に役立つ．

N の素因数がわかっていると，N−1 が素数であるかどうかの判定に役立つ．

N+1 と N−1 とでは別べつの定理で，両者で N+1 も N−1 も素数であることがわかれば双子素数の誕生である．詳細については，LeVeque [7] のなかの Lehmer による解説を参照せられたい．

整数論の実験に関する邦文の論説としては，高橋 [11]，田中 [12]，和田 [14] などがある．

数表 I. $\psi(x)-x$, $x=10^6(10^6)10^8$

−413.4	115.0	−0.02	−509.1	971.1
−350.4	575.1	121.7	850.2	−1460.5
18.9	728.1	824.2	−381.2	−561.2
−16.0	306.3	1970.1	779.3	607.4
−306.3	1311.8	−443.1	−674.6	−31.1
−546.0	106.1	−36.9	−142.2	718.8
2416.5	1074.6	1828.0	1883.0	−1821.2
−2348.4	−3434.5	−3297.1	−32.7	1526.5
1876.3	−604.3	−809.7	−842.1	−864.6
2410.7	2463.7	390.9	−1634.8	1303.5
1049.3	1711.5	962.4	258.6	−2168.5
−1202.8	360.6	−761.0	447.1	560.7
1663.1	−1920.1	−1866.8	358.8	−2146.7
−1959.5	383.5	2347.4	735.2	951.0
500.1	402.5	3716.0	2959.7	873.7
4228.7	1316.7	652.4	−1278.7	−1842.1
−91.8	2254.9	2797.8	2826.2	−685.3
−887.1	−956.4	−1466.5	152.0	−3935.9
−1625.7	−1088.1	−2384.4	−3487.7	74.1
671.2	211.7	1551.2	−2146.7	−1554.6

数表Ⅱ. $\psi_2(x)-Cx$, $x=10^6(10^6)10^8$

−7479.2	24505.9	19164.5	45105.3	40038.0
34405.6	29053.4	52207.2	68353.2	68436.1
70887.6	64830.7	49489.1	47092.9	52962.4
69026.3	66126.7	82575.1	79223.5	55116.8
66108.9	52517.4	55387.5	65621.9	75063.9
74930.1	62591.9	48911.7	47750.0	40509.9
46007.9	54302.7	34946.7	41768.8	37451.1
20713.9	56451.0	55201.5	60066.3	69762.9
70066.5	45285.2	31896.9	20525.7	18314.8
22086.5	21789.1	11954.7	6070.5	15868.8
−33863.4	−40276.9	−28819.3	−23253.3	−21594.8
−27076.7	−20708.4	−11092.0	−13454.9	−18287.1
−14885.5	−16610.7	−48343.6	−34551.2	−40585.2
−56196.3	−40070.3	−22547.9	−3829.6	19171.2
199.4	−43892.2	−20988.4	−4945.0	−19225.0
−7782.6	−7699.7	−5891.6	−20232.8	−35565.1
−54300.7	−26917.7	−30621.4	−29745.3	−33387.6
−32795.6	−20125.2	−17483.7	−17378.1	−23042.6
−17370.6	−6913.4	−6651.9	−9054.9	−5034.9
−9840.8	−17501.9	−20132.1	373.9	10286.9

参考文献

[1] R. P. Brent, Irregularities in the distribution of primes and twin primes, Math. Comp., 29 (1975), 43-56.

[2] P. Hagis, Jr., A lower bound for the set of odd perfect numbers, Math. Comp., 27 (1973), 951-953.

[3] G. H. Hardy and J. E. Littlewood, Some problems of partitio numerorum III, Acta Math., 44 (1922), 1-70.

[4] G. H. Hardy and E. M. Wright, An introduction to the theory of numbers, 4th. ed., Oxford, 1960.

[5] D. H. Lehmer, List of prime numbers from 1 to 10,006,721, Carnegie Institution, Washington, 1914; Hafner, New York, 1956.

[6] D. H. Lehmer, On the exact number of primes less than a given limit, Illinois J. Math., 3 (1959), 381-388.

[7] W. J. LeVeque, Studies in number theory, MAA, Prentice Hall, 1969.

[8] D. C. Mapes, Fast method for computing the number of primes less than a given limit, Math. Comp., 17 (1963), 179-185.

[9] H. Riesel, Lucasian criteria for the primality of $N = h \cdot 2^n - 1$, Math. Comp., 23 (1969), 869-875.

[10] B. Stubblefield, Greater lower bounds for odd perfect numbers, Notices A.M.S., 20 (1973), A-515.

[11] 高橋秀俊, 電子計算機と整数論, 数学, 15 (1963), 1-6.

[12] 田中穣, 整数論と電子計算機, 数学, 15 (1964), 168-172.

[13] B. Tuckerman, The 24th. Mersenne prime, Proc. Nat. Acad. Sci. U.S.A., 68 (1971), 2319-2320.

[14] 和田秀男, 整数論と計算機について, 数学, 26 (1974), 193-200.

[15] H.C. Williams and C.R. Zarnke, Some prime numbers of the forms $2A\cdot 3^n+1$ and $2A\cdot 3^n-1$, Math. Comp., 26 (1972), 995-998.