素数定理　数论　介绍　素数

进展简介

③

# 素数面面观 / 素数定理 100 年

290-297

黑川信重　王桂兰

## 1 素数

素数 2, 3, 5, 7, 11, 13, 17, ... 等，就是对自然数 1, 2, 3, 4, 5, 6, 7, ... 进行因子分解的时候，最后不能再分解的那些自然数 (但是， 1 不称为素数). 这就象分解宇宙的物质，终于找到原子和质子一样.

素数的研究是从 2500 年前古希腊时代开始的，特别地，毕达哥拉斯 (以毕达哥拉斯定理、即三平方定理而著名) 似乎是中心人物. 据说他们认为宇宙万物 (树，马，及人类等) 都是由素数产生的，而素数有无限个则确已证明了. (用反证法证明. 假设只有有限个素数 $p_1, p_2, p_3, \ldots, p_n$ 存在，那么对于自然数 $p_1 \times p_2 \times \cdots \times p_n + 1$, 不论用哪个素数都除不尽它 —— 这是因为用 $p_1, p_2, \ldots, p_n$ 中的任一个来除它都余 1, 与假设是矛盾的).

从那时开始的数学 (数论) 之梦就是写出无一遗漏地记载所有素数的 "全素数表". 这个梦想什么时候才能实现呢？比如，在本杂志『数学セミナ-』的 2096 年 1 月号上，完成 "全素数表" 连载，这种无法实现的事情能发生吗？如果能，那么不论是利用时间机器 (time machine) 还是其他什么，也绝对希望把那张表弄到手. 如果时间机器赶不及，那么只好寄希望于预订从现在起 100 年的『数学セミナ-』(1996 年 2 月号 - 2096 年 1 月号).

"全素数表" 对现在的地球数学来说是个梦，也许外星人能带来. 对素数附上颜色，"全素数表" 就是一个有如图 1 那样的涂有不同色彩的 "素数圆板"，从整体上看，不是闪烁着碧绿的美丽的光辉吗？

在写这篇文章之际，向在研讨素数及 ζ 函数的过程中，我们的同行者 ζ 研究所的诸位，表示感谢 —— 外星人柳川.

## 2 素数定理

虽然我们现在还见不到 "全素数表" 但关于素数是怎样分布的问题，从素数定

原题：素数いろいろ / 素数定理 100 年. 译自： 数学セミナ-, Vol. 34, No. 12, 1995, pp. 42-46.

理能大概知道．即使说素数的分布也还是含糊不清，我们现在仍可以先看一下到某个数为止的素数究竟有多少个．

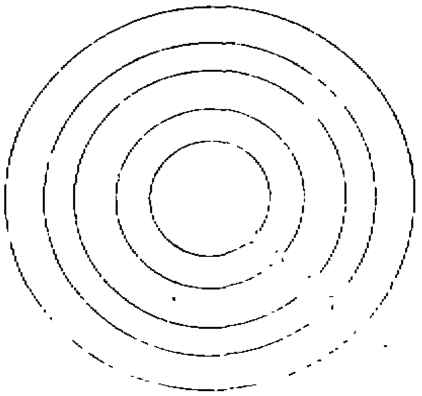

图 1

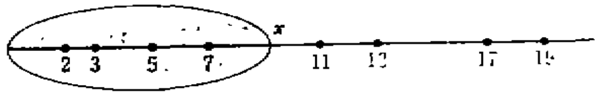


图 2

比如， 10 以下的素数有 2, 3, 5, 7 共 4 个 (见图 2).

我们数一下 100 以内的素数有： 2, 3, 5, . . . , 97, 正好 25 个．为了将这样的描述写成易懂的方式，我们将正数 $x$ 以下的素数的个数记为 $\pi(x)$ (这里的 $\pi$ 与圆周率无关，而是作为与素数 prime 的开头字母 $p$ 相对应的希腊字的首字母一样而使用的符号). 这样，可以简单地写为： $\pi(10)=4$ 及 $\pi(100)=25$. 这时

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

这里出现的 $\sim$ 是几乎相等的意思，准确的意思是说： "用 $\frac{x}{\log x}$ 去除 $\pi(x)$ 所得的商 (比), 随 $x$ 增大渐渐趋近于 1". 用另一种记号来写就是：

$$\lim_{x\to\infty} \frac{\pi(x)}{\left(\frac{x}{\log x}\right)} = 1.$$

这就是在距今 100 年前的 1896 年就已经被证明了的素数定理，是由 J · 阿达玛 (J. Hadamard) 和瓦莱普桑 (Ch. de la Vallée-Poussin) 彼此独立证明的.

在这个素数定理的证明中，使用了欧拉于 250 年前发现的 $\zeta$ 函数

$$\zeta(s) = \frac{1}{(1-\frac{1}{2^s})\times(1-\frac{1}{3^s})\times(1-\frac{1}{5^s})\times(1-\frac{1}{7^s})\times\cdots},$$

分母是取遍所有素数的一种乘积．把这个式子计算一下，得出：

$$\begin{aligned}\zeta(s) &= \frac{1}{1-\frac{1}{2^s}} \times \frac{1}{1-\frac{1}{3^s}} \times \frac{1}{1-\frac{1}{5^s}} \times \frac{1}{1-\frac{1}{7^s}} \times \cdots \\ &= \left(1+\frac{1}{2^s}+\frac{1}{4^s}+\frac{1}{8^s}+\cdots\right) \times \left(1+\frac{1}{3^s}+\frac{1}{9^s}+\cdots\right) \times \left(1+\frac{1}{5^s}+\cdots\right)\end{aligned}$$

$$\times\left(1+\frac{1}{7^s}+\cdots\right)\times\cdots$$
$$=1+\frac{1}{2^s}+\frac{1}{3^s}+\frac{1}{4^s}+\frac{1}{5^s}+\frac{1}{6^s}+\frac{1}{7^s}+\frac{1}{8^s}+\frac{1}{9^s}+\frac{1}{10^s}+\cdots.$$

从以上可以看出，所说的 $\zeta$ 函数具有两种表示 (关于所有素数的一种乘积以及关于全体自然数的一种和).

这是 $\zeta$ 函数最初被揭示的秘密. 如果使用这个关键点，立刻可以证明素数有无限个，不过这不是毕达哥拉斯当时的方法.

为此将 $s$ 代换成 1 考虑 $\zeta(1)$ 即可：

$$\frac{1}{1-\frac{1}{2}}\times\frac{1}{1-\frac{1}{3}}\times\frac{1}{1-\frac{1}{7}}\times\cdots$$
$$=1+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\frac{1}{5}+\frac{1}{6}+\frac{1}{7}+\frac{1}{8}+\frac{1}{9}+\frac{1}{10}+\cdots.$$

因为知道其右边无穷大 (如此加下去，没有尽头，不断增大), 所以左边也无穷大. 从

$$\boxed{1}+\boxed{\frac{1}{2}}+\boxed{\frac{1}{3}+\frac{1}{4}}+\boxed{\frac{1}{5}+\frac{1}{6}+\frac{1}{7}+\frac{1}{8}}$$
$$+\boxed{\frac{1}{9}+\frac{1}{10}+\frac{1}{11}+\frac{1}{12}+\frac{1}{13}+\frac{1}{14}+\frac{1}{15}+\frac{1}{16}}+\cdots$$
$$>\boxed{1}+\boxed{\frac{1}{2}}+\boxed{\frac{1}{4}+\frac{1}{4}}+\boxed{\frac{1}{8}+\frac{1}{8}+\frac{1}{8}+\frac{1}{8}}$$
$$+\boxed{\frac{1}{16}+\frac{1}{16}+\frac{1}{16}+\frac{1}{16}+\frac{1}{16}+\frac{1}{16}+\frac{1}{16}+\frac{1}{16}}+\cdots$$
$$=\boxed{1}+\boxed{\frac{1}{2}}+\boxed{\frac{1}{2}}+\boxed{\frac{1}{2}}+\boxed{\frac{1}{2}}+\cdots$$
$$=\infty\ (\text{無限大}).$$

而得知素数有无穷个 (因为如果素数只有有限个，左边也就变为有限的了).

将这一朴素的想法稍加精细化，就可以证明素数定理.

这时必要的 $\zeta$ 性质是：即使变量 $s$ 为复数，$\zeta(s)$ 仍有意义 (称为解析开拓), 特别是 $s$ 的实部 $\mathrm{Re}(s)$ 若为 1 以上，则 $\zeta(s)$ 不为零.

素数定理的精密化出现各种各样的情况，但现状则是，离开使用尚未解决的黎曼猜想 "如果 $\mathrm{Re}(s)>\frac{1}{2}$, 则 $\zeta(s)\neq 0$" 得到的结论：

$$\pi(x)=\int_2^x\frac{du}{\log u}+O(x^{1/2}\log x)$$

还相距甚远. 这里，用积分 (称为对数积分) 代替 $\frac{x}{\log x}$. 正如高斯和黎曼都注意到了的，是因为在比较误差的时候，此时的近似要好得多.

另外，记号 $O(x^{1/2}\log x)$ 意味着：误差 $|\pi(x)-\int_2^x \frac{du}{\log u}|$ 的大小在 $x^{1/2}\log x$ 的某常数倍以下．还知道不能根据比 $\frac{1}{2}$ 小的数 $a$，而取误差估计为 $O(x^a)$ 的形式．在此种意义上．如果证明了黎曼猜想，素数定理的精密化也就迎来了大体的完成．

但遗憾的是，至今为止，连误差取为 $O(x^{1-1/100000000})$ 的形式也没有完成（不论 1/100000000 取怎样小的正数）．

黎曼猜想是 $\zeta$ 函数的美的象征，是生存的原动力所在．从"全素数表"看，黎曼猜想也许非常简单易懂．我们寄希望于即将开始的 21 世纪．

## 3 各种素数的分布

关于素数全体的分布情况的研究，目前也就到素数定理。详细看一下素数的形式和特性将是怎样的呢？请看下面的三个例子：

（Ⅰ）$p=4n+1$（$n$ 是自然数）的形式，（例）$p=5,13,17,\ldots$；

（Ⅱ）$p=n^4+1$ 的形式，（例）$p=2,17,257,\ldots$；

（Ⅲ）$p=2^n-1$（梅森素数）的形式，（例）$p=3,7,31,\ldots$．

稍微计算一下即可看出．无论哪种形式，其中的素数都很多．

我们知道，对应（Ⅰ）式的素数个数是无限的，已于 1837 年由狄利克雷（Dirichlet）证明了．但对应（Ⅱ），（Ⅲ）式、素数有无限个的问题，至今为止尚未证明．

这时、要考虑与原素数定理相似之处，只要研究公式

$$\pi(x,4n+1)=[x\text{ 以下的素数 }p\text{ 中，满足 }4n+1\text{ 条件的素数的个数}],$$

$$\pi(x,n^4+1)=[x\text{ 以下的素数 }p\text{ 中，满足 }n^4+1\text{ 条件的素数的个数}],$$

$$\pi(x,2^n-1)=[x\text{ 以下的素数 }p\text{ 中，满足 }2^n-1\text{ 条件的素数的个数}].$$

将狄利克雷（Dirichlet）的结果稍加严密化即为

（Ⅰ）$\pi(x,4n+1)\sim\frac{1}{2}\cdot\frac{x}{\log x}\quad(x\to\infty)$.

也就是说，$x$ 以下的素数（$\pi(x)$ 个）中，按比率有一半是用 4 除余 1 的素数，因此其余一半是用 4 除余 3 的素数（但是 2 是例外）：

$$\pi(x,4n+3)\sim\frac{1}{2}\cdot\frac{x}{\log x}\quad(x\to\infty).$$

狄利克雷将素数溶于形形色色的 $\zeta$ 函数中，再从中抽出个性，从而导出这样的结果（对 $p=an+b$ 的形式时也是如此）．

再有，对（Ⅱ），（Ⅲ）从概率上考虑，可得出下面的猜想：

（Ⅱ）$\pi(x,n^4+1)\sim(2.6789\ldots)\cdot\dfrac{x^{1/4}}{\log x}\quad(x\to\infty)$；

（Ⅲ）$\pi(x,2^n-1)\sim(2.5695\ldots)\ \log\log x\quad(x\to\infty)$.

其中，直到 $x$ 相当大的时候，研究（Ⅱ）都很符合猜想．关于（Ⅲ）式，虽例子不多（现在知道的有 3, 7, 31, …, $2^{859433}$ -1 共 33 个）、但可以认为基本符合猜想．证明（Ⅱ），

(Ⅲ) 式的论据不足．素数分布的密度，按 (Ⅰ), (Ⅱ), (Ⅲ) 的顺序，逐渐变得稀少，随着素数分布密度的变稀，边计算边证明就更困难了．

今后，按公式的形式，将 (Ⅰ) 式称为一次型，(Ⅱ) 式称为多项式型，(Ⅲ) 式称为指数型．比如：$p = an + b$ 称一次型，$p = an^2 + bn + c$ 称多项式型．在 (Ⅰ) 的情况下，由狄利克雷的结果证明了素数定理，其他的情况则仅仅被认为是猜想．

猜想的 (Ⅱ) 例子：

$$\begin{cases} \pi(x, n^2+1) \sim (1.3728\ldots) \cdot \dfrac{x^{\frac{1}{2}}}{\log x} \quad (x \to \infty), \\ \pi(x, n^2+n+41) \sim (6.6395\ldots) \cdot \dfrac{x^{\frac{1}{2}}}{\log x} \quad (x \to \infty). \end{cases}$$

另外，(Ⅱ) 和 (Ⅲ) 也有变型版本存在．下面看几种变型．

(Ⅱ)的变型①：孪生素数

设 $\pi_2(x) = [x$ 以下的素数 $p$ 中，$p+2$ 也是素数的素数个数$]$，形成象 (3,5), (5,7)、(11,13) 等形式的孪生素数．猜想为：

$$\pi_2(x) \sim C \cdot \frac{x}{(\log x)^2} \quad (x \to \infty).$$

这点，在其他的情况虽然也相同，但常数 $C$ 可以准确地计算，现在的场合就是

$$C = 2 \times \left(1 - \frac{1}{(3-1)^2}\right) \times \left(1 - \frac{1}{(5-1)^2}\right) \times \left(1 - \frac{1}{(7-1)^2}\right) \times \cdots = 1.3203\ldots,$$

其中无限积为与 3 以上的素数 3,5,7,... 有关的乘积．素数的倒数之和等于无穷大 (这从 $\zeta(1) = \infty$ 可见)．但是孪生素数的倒数之和是有限的，这已在 1919 年由布朗证明过．计算一下，$(1/3 + 1/5) + (1/5 + 1/7) + \cdots = 1.9021\ldots$，我们知道孪生素数很少．但是并没有证明它们有无穷个 (说少比证明无限个更容易)．

(Ⅱ)的变型②：椭圆曲线及自守形式的情况

关于椭圆曲线及自守形式，在这里由于篇幅的关系，不能作深入说明，但无论哪一个对费马猜想的解决都起了重要的作用．请参看加藤和也先生的『解决！费马的最终定理 / 现代数论的轨迹』(日本评论社，1995 年)．

设 $E$ 为有理系数的椭圆曲线且不带虚数的乘法．(例☆) 如果用方程式 $x^3 - x^2 = y^2 - y$ 定义的曲线．这时若设 $L(s, E) = \sum\limits_{n=1}^{\infty} a(n, E) n^{-s}$ 为其 $\zeta$ 函数，则对 (充分大的) 素数 $p$ 有

$$a(p, E) = 1 + p - \#\widetilde{E}(E_p)$$

成立．在这里

$$\#\widetilde{E}(E_p) = [\text{mod } p \text{ 的解的个数}] + 1$$

(加 1 是由于 $(\infty,\infty)$ 也看作是椭圆曲线上的点). 此时，考虑： $\pi_E(x)=[x$ 以下的素数 $p$ 中，满足 $a(p,E)=0$ 的素数的个数] (这样的 $p$ 称为超奇异的). 猜想有下述结果成立：

$$\pi_E(x)\sim (\text{常数})\cdot x^{1/2}/\log x \quad (x\to\infty),$$

(朗. 托洛塔， 1976 年). 从而应该与 $\pi(x,n^2+1)$ 等有同样程度的分布. 这里，应该注意之点是 $\pi_E(x)$ 比 $\pi(x,n^2+1)$ 等情况的研究更进一步，当 $x\to\infty$ 时， $\pi_E(x)\to\infty$. 亦即证明了满足 $a(p,E)=0$ 的 $p$ 有无限个 (Erdös,1987 年)(例☆). 此时超奇异的 $p$ 为：19, 29, 199, 569, 809,... (个位数为 9).

椭圆曲线 $E$ 的说法按照解决费马猜想的 Wiles 的定理、可以改为自守形式 $f=\sum_{n=1}^{\infty}a(n,f)q^n$ 的说法 (但是，现在 "$E$ 的导数不含平方因子" 这条件是必要的). 在这里， $a(n,f)=a(n,E)$ 成立、 $\zeta$ 函数同样：

$$L(s,f)=\sum_{n=1}^{\infty}a(n,f)n^{-s}=\sum_{n=1}^{\infty}a(n,E)n^{-s}=L(s,E).$$

从而、若令

$$\pi_f(x)=[\text{在 } x \text{ 以下的素数 } p \text{ 中，满足 } a(p,f)=0 \text{ 的素数的个数}],$$

则 $\pi_f(x)=\pi_E(x)$ 成立. 对 $\pi_E(x)$ 的说明可以解释为关于 $\pi_f(x)$ 的说明. 比如、与 (例☆) 的 $E$ 相对应的 $f$ 为：

$$f=q\prod_{n=1}^{\infty}(1-q^n)^2(1-q^{11n})^2=q-2q^2-q^3+2q^4+q^5+\cdots,$$

(请确认 $q^{19}$ 及 $q^{29}$ 的系数变为零). 我们把这样的说法推广到阿贝尔簇，代数簇，及多变量的自守形式，恐怕也很有意思.

(Ⅲ) 的变型：阿贝尔的问题 (1828 年)

对于自然数 $a=2,3,\ldots$，考虑

$$\begin{aligned}\pi^a(x)&=[\text{在 } x \text{ 以下的素数 } p \text{ 中，满足 } a^p\equiv a \bmod p^2 \text{ 的素数的个数}]\\&=[\text{在 } x \text{ 以下的素数 } p \text{ 中，满足 } a'(p)=0 \text{ 的素数的个数}].\end{aligned}$$

但是， $a'$ 是 "绝对微分"

$$a'(p)=\left[\frac{a^p-a}{p} \bmod p\right].$$

这时，可以猜想

$$\pi^a(x)\sim\log\log x \quad (x\to\infty),$$

(这样的素数，在费马猜想的第一种情况下，也可以考虑作为维富利的条件). 关于这点，对不太大的 $a$、有计算的实例，比如 $a=2$ 时， $p=1093$ 及 3511(无论哪个都可以

手算), $a=3$ 时, 也可找到 $p=11$ 及 1006003($p=11$ 是雅可比 (Jacobi) 发现的) [关于「数的微分」, 请参看伊藤康隆先生的 [Fermat 商和关于「数的微分」, 『数理解析研究所讲录』 **810**(1992), p. 324–341].

另外, $2'(1093)=0, 2'(3511)=0$ 等, 微分变为 0, 这样作下去, 2 的图形允许变为如图 3 那样.

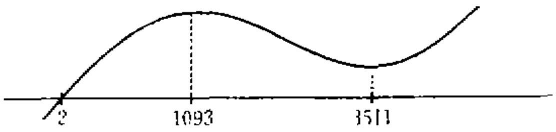


图 3

从在 "一元域" $F_1$ 上考虑数学这种绝对数学的观点出发, 整数 $0, \pm1, \pm2, \ldots$ 可以称为 $F_1$ 系数的多项式。这样, 素数 $2, 3, 5, 7, \ldots$ 也应该构成某种多项式, 而且, 毫无疑问, 在黎曼猜想的证明等方面发挥巨大作用. [关于绝对数学请看: 「绝对数学的探求: 1 和 2 和 3 」『 Springer-Science 』第 10 卷 2 号 ( 1995 ), p.6-10 ].

**关于定理的注记:**

这里出现的常数各个都具有数论的结构. 如果使用平方剩余记号 $(p/q)$, 则有如下的表示:

$$2.6789\ldots = \prod_{p\ \text{奇素数}} \left(1 - \frac{\left(\frac{-1}{p}\right) + \left(\frac{2}{p}\right) + \left(\frac{-2}{p}\right)}{p-1}\right),$$

$$1.3728\ldots = \prod_{p:\ \text{奇素数}} = \left(1 - \frac{\left(\frac{-1}{p}\right)}{p-1}\right),$$

$$6.6395\ldots = 2 \times \prod_{p:\ \text{奇素数}} \left(1 - \frac{\left(\frac{-163}{p}\right)}{p-1}\right).$$

在梅森素数的分布中出现的常数是:

$$2.5695\ldots = \frac{e^{\gamma}}{\log 2},$$

其中

$$\gamma = \lim_{n\to\infty}\left(1 + \frac{1}{2} + \cdots + \frac{1}{n} - \log n\right) = 0.577\ldots$$

是欧拉常数.

## 4 素数的进化

到现在为止，我们见到了 2, 3, 5, 7, ... 等普通的素数．但是“素数”的概念在不断地进化着．任何物体进行分解最后所得到的元素称为“素数”．

众所周知，有两种考虑方法．即从环(可以进行加减乘(除)的「数」的集合)$R$ 中取出不能分解为积的“素数”全体 $P(R)$，以及从群(可以进行乘除的「数」的集合)$G$ 中取出不是其它元素的乘积的“素数”全体 $P(G)$[详见：黑川写的「素数的一般化和 $\zeta$ 函数」，『数学セミナ-』，1993 年 10 月号，11 月号]．

无论哪种情况都能构成 $\zeta(s)$，由此可以证明“素数定理”．但是在后者的情况，已经知道的要精确得多，证明了黎曼猜想的类似结论，并且在与(II)非常相似的分布的情况，完成了素数定理的证明(胜田 - 砂田，菲利普斯 - 萨尔纳库，1987 年)．从几何的角度看，前者的情况“素数”是对“点”的，而后者的情况不同，被看作“直线”及“圆”．[请看砂田利一先生的「素数和测地线和鼓声」，『数理科学』，1994 年 8 月号，pp. 20–24]．从而，为了在通常素数的情况下，也按照群 $G$ 而解释为 $\zeta(s)=\zeta(s,G)$，象图 1 那样看素数全体的图 1 比图 2 要好．

这样进化了的素数其自身就饶有兴味，无疑对原来素数的研究也会带来深入的思考。

素数今后将向何处去呢？等待素数未来的将是什么呢？毫无疑问，素数走到了终点一定也就是数学的目的地(到达数学也将完结的地方)．人类的进化果真能够赶超素数 $\zeta(s)$ 的进化吗？！

(王桂兰，郑玉颖 译　陈治中 校)