

生活与科学文库

从素数发现到
电脑计算

素数的奥秘

生活与科学
文库

〔日〕堀场芳数 著

分数和小数
复数的出现
魔方数和三角阵
偶数和奇数
自然数的产生
素数与人类社会

科学出版社

生活与科学文库

素数的奥秘

——从素数发现到电脑计算

〔日〕 堀場芳数 著

丁 树 深 译

科 学 出 版 社

「素数の不思議」 堀場芳数

© Yoshikazu Horiba

All rights reserved

First published in Japan in (1994) by Kodansha Ltd. Tokyo

Chinese version published by Science Press, Chinese Academy of Sciences

Under license from Kodansha Ltd.

本书据日本讲谈社 1994 年第 14 次印刷版译

图字:01-1999-3300 号

图书在版编目(CIP)数据

素数的奥秘/[日]堀場芳数著;丁树深译.

-北京:科学出版社,2000

(生活与科学文库)

ISBN 7-03-008324-5

I. 素… II. ①堀… ②丁… III. 素数-普及读物 IV. O156.2

中国版本图书馆 CIP 数据核字(2000)第 03899 号

科 学 出 版 社 出 版

北京东黄城根北街 16 号

邮政编码:100717

北京双青印刷厂印刷

科学出版社发行 各地新华书店经销

*

定价: 10.00 元

(如有印装质量问题,我社负责调换〈环伟〉)



素数是什么数？对我们的日常生活而言，素数也许是无关系要的数吧？！

从古希腊欧几里得(Euclid, 公元前 300 年左右, 生卒年不详)开始, 自古以来就有很多数学家研究素数, 但在现代数学中, 素数至今仍隐藏有未知的部分。因此, 在素数起着重要作用的整数论中, 目前依然留存一些有待开拓的研究课题。

当然, 这本小册子不能完全包括素数的全部内容, 但概括介绍素数研究领域的最新进展是必要的。所以, 本书叙述素数奥秘是很有意义的。

自然数, 即 $1, 2, 3, \dots$ 正整数是一无限延伸(扩展)的数列, 其中, 除 1 以外大于 2 的每个数都有几个约数。但是, 这其中还应有一些除 1 和它本身以外, 没有其他约数(不能被其他正整数整除)的数, 例如, $2, 3, 5, 7, 11, 13, 17, 19, \dots$ 以及无穷多个这类数。

这样的正整数, 即不可约数, 被称为素数。除 2 以外素数皆为奇数。当然, 2 位数以上尾数为 5 的奇数不是素数。简言之, 素数是无穷尽的数。

素数的英文名称为 prime number, 英文字典中“prime”有最初的、首要的、原始的以及原有的、根本的等解释。

明治时代的日本数学家认为, “根本的”译意有元素及要素之类的含意, 所以将“prime number”译为素数。

素数是数的根源。这样, 一切自然数是素数或素

数乘积所构成的合数,而合数可分解为素数因子(数),并可转化为素数之积。例如, $210=2\times 3\times 5\times 7$ 。

本书在说明素数过程中,依次列举出与素数演化相关的几位数学家。欧几里得是最早研究素数的开拓者,接着有 Gauss、欧拉、黎曼、梅森、切比雪夫、狄利克雷、阿达马、普桑和塞尔伯格等数学家。此外,还有对数学研究有兴趣的费马,以及天文学家兼地理学家埃拉托色尼等光彩夺目的历代名人。书中还穿插一些诙谐故事,通俗易懂地叙述了这些科学家们的人品和业绩。

当然,目前在电脑时代不可越过电脑讨论素数。有关这方面的情况,书中也都略有提及。

本书读者中哪怕只有少数人能体会到:数学原来是如此智慧而奇妙的一门学问,这对笔者来说也是最大的欣慰了。

堀場芳数

1994年春



前 言

第一章 数的起源与发展	(1)
§ 1.1 数表示什么	(1)
§ 1.2 自然数的产生	(2)
§ 1.3 上古时期的数字	(7)
§ 1.4 零(0)和阿拉伯数字的诞生	(9)
§ 1.5 分数和小数	(14)
§ 1.6 负数的出现	(16)
§ 1.7 有理数和无理数	(19)
§ 1.8 虚数的出现和复数	(20)
第二章 自然数的各种使用方法	(25)
§ 2.1 三角形数和四角形数	(25)
§ 2.2 毕达哥拉斯数, 完全数和亲和数	(27)
§ 2.3 魔方数和三角阵	(31)
§ 2.4 随机数表(模拟随机数表)	(33)
§ 2.5 阶乘、平方和立方	(50)
第三章 约数、倍数和素数	(55)
§ 3.1 欧几里得和素数	(55)
§ 3.2 约数和倍数	(58)
§ 3.3 5的倍数, 九去法, 末两位为4的倍数	(59)

§ 3.4	偶数和奇数	(61)
§ 3.5	公约数和最大公约数	(63)
§ 3.6	公倍数和最小公倍数	(65)
§ 3.7	埃拉托色尼的素数筛选	(66)
§ 3.8	孪生素数	(70)
第四章	梅森素数和费马素数	(71)
§ 4.1	梅森素数	(71)
§ 4.2	梅森小传	(86)
§ 4.3	与梅森深交的笛卡儿	(87)
§ 4.4	梅氏教堂中聚集的数学家们	(89)
§ 4.5	费马素数	(94)
§ 4.6	费马的兴趣是研究数学	(96)
第五章	素数分布	(98)
§ 5.1	10 万以内的素数表	(98)
§ 5.2	素数的确认	(127)
§ 5.3	素数的分布	(131)
§ 5.4	高斯预料的素数定理	(133)
§ 5.5	狄利克雷和等差级数定理	(136)
§ 5.6	切比雪夫定理	(137)
§ 5.7	证明素数定理的人们	(139)
§ 5.8	素数记忆窍门	(141)
第六章	素数的各种研究	(142)
§ 6.1	约数化后的素数因数分解	(142)
§ 6.2	欧拉和素数	(161)
§ 6.3	素数与人类社会	(168)
§ 6.4	待发现的素数和合数	(169)
§ 6.5	$n^2 - 1$ 中有素数吗	(183)
§ 6.6	$4n \pm 1$ 和素数的关系	(193)

§ 6.7 关于 $6n \pm 1$ 型的素数	(196)
§ 6.8 密码在一般商务中的应用	(197)
第七章 电脑挑战素数	(199)
§ 7.1 求素数的电脑程序	(199)
§ 7.2 数表及其电脑程序	(210)
§ 7.3 素数因数分解的电脑程序	(220)
结束语	(230)
参考书目	(231)

第一章

数的起源与发展

§ 1.1 数表示什么

在南非部落中，数只有 1，2 和很多三种。日本在原始时期也只有 1 个、2 个和很多，或者 1 个和很多个这类数。

远古时期还没有数物件的数词，给孩子东西时，只有 1 个和许多个之间有区别。

古时候日本没有数字，但却有数词，即用在数数时说的一个、二个、三个、四个、五个、六个、七个、八个、九个、十个等等。后来又附加日本数词字尾，从而构成日本专用数词。

另外，日本数词还有音读一说，音读是引用中国汉语数字拼读而产生的日语数词（的）发音。

那么，数究竟是什么呢？首先，数表示物品的数目，也就是说，数一数物品有多少。其次，数表示顺序先后以及它们之间的大小关系，而现在又从物体长度、重量、体积和钟点时刻等扩展到物体位置的表达。

现在，借助阿拉伯数字（下同），即印度·阿拉伯数字或算用数字，多大的数都可以表示。回顾我们祖先在数方面所付出的艰辛，可以说是十分有意义的。

§ 1.2 自然数的产生

如前所述，最早的数是从需要数一数物品的个数开始的，并由此产生 1, 2, 3, … 等自然数，换句话说，产生的是正整数。虽然世界各地语言不同，数字读法也各不一样，但无论在哪里、哪个国家，数的产生都是相同的。

现在，借助含零 (0) 的阿拉伯数字，无论多大的数都可用这 10 个数字表示，甚至在没有阿拉伯数字的远古时期，在印度还有个、十、百、千、万、亿、兆、京、……那样大的数目词，而且一直用来表示大的自然数。

众所周知，印度的自然数是万进制数字，并且是“几千几百几十几”那种逢千位数进 1 位的，而欧美各国的自然数数词，像“壹佰贰拾叁”那样，是逢 3 位数进 1 位的千进制。

在日本和欧美国家都有非常大的自然数，大的单位在日本是万进位数字，在欧美是千进位数字。

为备用参考起见，表 1-1 列出中国、日本和欧美的数词对照表。由中国传入日本的数，当然为万进制*。

* 对表 1-1 略作改编，万进制可一目了然，如表 1-2 所示——译者注

表 1-1 中国、日本和英美数词

10^0	一	one	10^{23}	千垓		10^{46}	百载	
10^1	十	ten	10^{24}	秭	古称为秭	10^{47}	千载	
10^2	百	hundred	10^{25}	十秭		10^{48}	极	
10^3	千	thousand	10^{26}	百秭		10^{49}	十极	
10^4	万	ten thousand	10^{27}	千秭		10^{50}	百极	
10^5	十万		10^{28}	穰		10^{51}	千极载	
10^6	百万	million	10^{29}	十穰		10^{52}	恒河沙	
10^7	千万		10^{30}	百穰		10^{53}	十恒河沙	
10^8	亿	hundred millions	10^{31}	千穰		10^{54}	百恒河沙	
10^9	十亿	美、法 billion	10^{32}	沟		10^{55}	千恒河沙	
10^{10}	百亿		10^{33}	十沟	美、法 decillion	10^{56}	阿僧祇	
10^{11}	千亿		10^{34}	百沟		10^{57}	十祇	
10^{12}	兆	美 trillion 英、德 billion	10^{35}	千沟		10^{58}	百祇	
10^{13}	十兆		10^{36}	涧		10^{59}	千祇	
10^{14}	百兆		10^{37}	十涧		10^{60}	那由他	英、德 decillion
10^{15}	千兆		10^{38}	百涧		10^{61}	十那由他	
10^{16}	京		10^{39}	千涧		10^{62}	百那由他	
10^{17}	十京		10^{40}	正		10^{63}	千那由他	
10^{18}	百京	英 trillion	10^{41}	十正		10^{64}	不可思议	
10^{19}	千京		10^{42}	百正		10^{65}	十不可思议	
10^{20}	垓		10^{43}	千正		10^{66}	百不可思议	
10^{21}	十垓		10^{44}	载		10^{67}	千不可思议	
10^{22}	百垓		10^{45}	十载		10^{68}	无量 大数	

表 1-2 中国和日本大数词的万进制换算

名称		数值及其换算
中、日	美、法 英、德	
万	ten thousand	$10^4 = 10^4 \cdot 10^0$
亿	hundred millions	$10^8 = 10^4 \cdot 10^4$ (万万)
兆	美 trillion 英、德 billion	$10^{12} = 10^4 \cdot 10^8$ (万亿)
京		$10^{16} = 10^4 \cdot 10^{12}$ (万兆)
垓		$10^{20} = 10^4 \cdot 10^{16}$ (万京)
秭		$10^{24} = 10^4 \cdot 10^{20}$ (万垓)
穰		$10^{28} = 10^4 \cdot 10^{24}$ (万秭)
沟		$10^{32} = 10^4 \cdot 10^{28}$ (万穰)
涧		$10^{36} = 10^4 \cdot 10^{32}$ (万沟)
正		$10^{40} = 10^4 \cdot 10^{36}$ (万涧)
载		$10^{44} = 10^4 \cdot 10^{40}$ (万正)
极		$10^{48} = 10^4 \cdot 10^{44}$ (万载)
恒河沙		$10^{52} = 10^4 \cdot 10^{48}$ (万极)
阿僧祇		$10^{56} = 10^4 \cdot 10^{52}$ (万恒河沙)
那由他	英、德 decillion	$10^{60} = 10^4 \cdot 10^{56}$ (万阿僧祇)
不可思议		$10^{64} = 10^4 \cdot 10^{60}$ (万那由他)
无量无数		$10^{68} = 10^4 \cdot 10^{64}$ (万不可思议)

我们先稍离正题，说一说自然数的计算。

“乘法口诀”也叫“九九口诀”，是乘法运算的基础。它是公元前首先在中国出现的，但由谁发明却毫无记载。乘法口诀是从 1 至 9，每 2 个数相乘而得，从“一一得一”开始到“九九八十一”止，故称之为“乘法九九”，而且一直流传至今。

与此相应，也有称之为“除法口诀”的“除法九九”。笔者念小学时期，在珠算私塾中也背通过“二一添作五”、“逢二进一”之类难懂的除法口诀。

可是，现如今珠算私塾里的除法运算，在日本却被称为“龟井算”或“百川龟井算”，并且一直使用乘法口诀进行除法运算。

有关百川和龟井的传说很多，所以先来作个介绍。

百川治兵卫（1580～1638）是距今350年前江户初期的数学家，即日本算学家。当时的大部分日本算学家认为，算盘先生是不务正业的算学家。

从毛利重能（17世纪，生卒年不详）的《除算书》和吉田光由（1598～1672）的《尘劫记》，到后来的大正末期，使用算盘作除法运算，一直采用前面介绍过的“除法九九”口诀。

龟井算除法是采用“九九口诀”的除法运算，这种运算方法和笔算一样，得商后从被除数减去除数乘商数之积。

这种方法由谁发明尚不能肯定，有人说自从1655年（明历元年）百川治兵卫写了《新编诸算记》后，这种方法就广为流传下来了。

但还有另一种说法，此前25年的1630年（宽永7年），百川治兵卫被发配佐渡岛，在流放途中，经过新泻一带时曾讲授过这种除法运算方法。此间还流传一段有趣的故事。

传说大约在350年前，大坂有一位叫百川一算的珠算先生，他在堂岛开办了一所私塾，为附近的人们讲授珠算。

那时，大粮店老板中的珠算能手都前来学习。其中有一年，稻谷丰收，市场粮价下跌，因而粮店遭受了巨大损失。因此，百川一算向当地粮店老板们借了一大笔钱，并且消失得无影无踪了。过了一段时间之后，一大批乞丐从全国各地蜂涌前来大坂，而且异口同声地扬言：“东北地带粮食收不上来啦！”。这样大造声势后，粮价不断上涨，粮店老板当然获利可观。

实际上，这场骚乱是百川一算一手策划的。乞丐们从百川一算那里拿到钱后，专门被派来宣传闹事的。后来这件事被官方查明，官府决定把百川一算流放到佐渡岛。

流放途中，在到达新泻时，海上风浪大作，船被迫停泊在新泻。当时，一位叫龟井律平的看守对百川一算态度十分诚恳而热情。

龟井律平对珠算颇着迷，甚至在梦中都在练习打算盘。得知这种情况后，百川一算想：“我若死在佐渡岛，自己搞出来的一套运算方法必将与自己同归于尽”，于是就把使用“乘法九九”的除法运算传授给龟井律平了。最后补充一句话说：“跟流放到岛上的罪犯学习，实属对上级不恭敬，故请慎重。”

此后，龟井律平把龟井算传授给人们了，为缅怀百川一算的功德，取名为百川龟井算。

这个故事没有确凿证据可查，但却一直在新泻一带流传，这也许是对当时政权的一种反抗。

这位叫百川一算的人实际就是百川治兵卫，若果真如此，那么这个故事也是很有道理的。

§ 1.3 上古时期的数字

非常遗憾，日本根本就没有固有数字。远古时代，世界各地表示数的方法是共同的，即以物代替数字，并用木棍和小石块之类的多少来表达数的大小。

这种方法实际上是一种“一一对应”法。据说，后来也采用身旁的一些其他物品代表数目，例如可以用狮子的头代表 1，鹭的翅膀代表 2 等。然而，新几内亚一带的土著居民却用左手小手指代表 1，无名指为 2，中指为 3，食指为 4，拇指为 5，等等。

可是，在南美洲古代的印加帝国和古代的日本冲绳，则利用绳扣表示“数”。

更早些时候，在中美洲的玛雅部落里采用 $\bullet$ 和 $-$ 代表数，而且 $\bullet$ 代表 1， $\bullet\bullet$ 为 2， $\bullet\bullet\bullet$ 为 3， $\bullet\bullet\bullet\bullet$ 为 4， $-$ 为 5， $\bullet-$ 为 6， $\bullet\bullet-$ 为 7， $\bullet\bullet\bullet-$ 为 8， $\bullet\bullet\bullet\bullet-$ 为 9， $-$ 为 10，并且是二十进制。

据说， $\bullet$ 代表女性， $-$ 代表男性等等。

按照这种表示，9 为 $\bullet\bullet\bullet\bullet-$ 。根据伊斯兰教教规，丈夫最多可有四位妻子，玛雅数字也是在一上最多放 4 个 $\bullet$ ，这可说是毫无关系的生拉硬扯，或者是偶然巧合的趣闻。

笼统看来，希腊数字 $I, II, III, IIII, \Gamma, \Pi, \dots, \Delta$ ，是表示 1~10 的数字，并且是逢 5 进 1 的十进制数。罗马数字 $I, II, III, IV, V, VI, \dots$ 也是逢 5 进 1 的十进制数。

另外还有巴比伦的楔形数字，如图 1-1 所示，也是十进制数字。

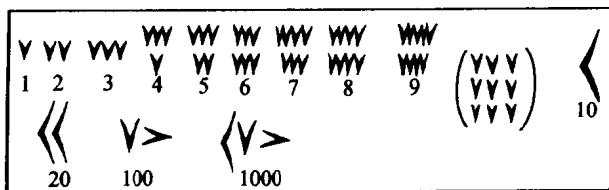


图 1-1 巴比伦楔形数字

阿拉伯数字尚未传入欧洲之前，欧洲一直采用上述罗马数字。作为钟表字盘的数字和文件、著作中的装饰数字，罗马数字一直延用至今。

在希腊，还有采用希腊字母 α , β , γ , δ , ... 表示 1, 2, 3, 4, ... 的时代。

现在麻将牌上所见到的埃及数字，如图 1-2 所示，也是十进制数字。

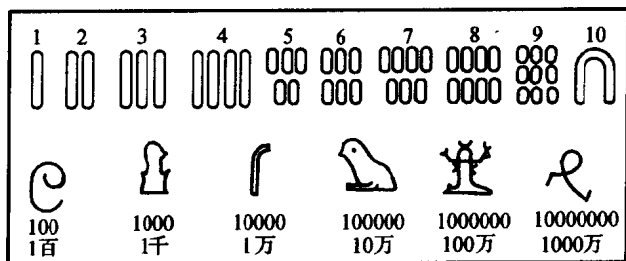


图 1-2 古埃及数字

那么，中国创造的汉语数字流传到日本是很久很久以前的事情了，但只是在数字和文字横着写以后，江户时期的数学，即日本算学才得以繁荣。在牛顿 (1642~1727) 和莱布尼茨 (1646~1716) 同一时期，日本算学的微积分研究仍采用中国的汉语数字计算，

实在令人惊叹。

中国的汉语数字也是十进制，印度的大的数字也是十进制，并且是由中国经印度流传到日本的。

为方便参考，用希腊数字和罗马数字写出 365，如图 1-3 所示。

希腊数字 $\Gamma = 5$ $\Delta = 10$ $\text{P} = 50$ $\text{H} = 100$
HHHP Δ Γ

罗马数字 $V = 5$ $X = 10$ $L = 50$ $C = 100$
CCCLXV

图 1-3 希腊数字和罗马数字书写的 365

§ 1.4 零(0)和阿拉伯数字的诞生

这一节的标题，在“BLUE BACKS”系列丛书的《零的奥秘》小册子中，作者已有详述，因此这里只简单提一下。

公元 5 世纪，数学研究在印度已十分盛行，大数学家阿耶波多 (Aryabhata, 476~530 前后)、婆罗摩笈多 (Brahmagupta, 598~660 前后) 等人当时非常活跃。尔后，婆什迦罗二世 (Bhaskara II, 1114~1185) 在这方面也进行过探索。

因此，在公元 500~600 年前后，零 (0) 的使用和进位数字就同现在一样。0 表示太阳，最初用黑色 •，后来就用 0 表示。

但是，也有人认为 0 是鬼数。因为

$$2+0=2, 0+3=3, 4-0=4, 0-5=-5$$

$$6\times 0=0, 0\times 7=0, 0\div 8=0$$