素数分布与哥德巴赫猜想

素数分布与哥德巴赫猜想

潘承洞

山东科学技术出版社

一九七九年·济南

素数分布与哥德巴赫猜想

潘承洞

*

山东科学技术出版社出版
山东省新华书店发行
山东新华印刷厂潍坊厂印刷

*

787×1092毫米32开本 3.875印张 74千字
1979年12月第1版 1979年12月第1次印刷
印数：1—20,000

书号 13195·15 定价 0.42元

出版者的话

数论是数学的一个古老分支，国内外许多著名数学家，都从事过数论问题的研究。数论的研究方法及其成果，对数学的其他分支及自然科学的不少学科一直起着积极的推动作用。近二十多年来，随着科学技术的发展，数论在计算数学等方面又有了日渐深入的研究，受到科学技术工作者的普遍重视。

自我国数学家陈景润研究员发表了关于哥德巴赫猜想的著名论文以来，在国内外数学界引起了强烈的反响，也使我国的许多科技工作者感到了极大的兴趣，希望对哥德巴赫猜想等数论问题能有较深入的了解，掌握一些有关方面的基本知识。为了帮助读者达到这一目的，我们请山东大学潘承洞教授编写了《素数分布与哥德巴赫猜想》这本书。

潘承洞教授对哥德巴赫猜想、素数分布、零点密度分布等问题的研究，有很深的造诣。早在1962年，他首次得到了关于哥德巴赫猜想的(1,5)的定量结果，此后，又改进为(1,4)。近几年来，他与陈景润研究员、王元研究员等关于哥德巴赫数、均值定理等问题的研究，被国际数学界公认为第一流的成果。

本书以数论中的素数分布与哥德巴赫猜想这两个著名问题为中心，深入浅出地介绍了数论中的一些基本概念以及研究这两个问题的主要方法，简要地叙述了哥德巴赫猜想的历史与现状。通过这些，将使读者对数论的研究内容有初步的了解，也将为数论的进一步研究奠定基础。

本书在编写过程中，承中国科学院王元教授及山东大学数学系裘卓明、于秀源同志提出宝贵意见，谨此致谢。

1979年6月

目　录

第一章　哥德巴赫猜想概述

人们经常要同各种数字打交道，从日常生活到最新的尖端科学技术都离不开数．我们最熟悉和用得最多的是1，2，3，4，5，…这些正整数，它们也叫作自然数．研究正整数的性质，特别是整除性，是一件十分重要而有趣的事，它的性质非常丰富，至今还没有被人们所完全认识．“数论”就是研究正整数性质和规律的一门学问．

我们把那些可以被2整除的数叫作偶数，如2，4，6，8，…剩下的那些正整数就叫作奇数，如1，3，5，7，…这样，所有的正整数就被分成了偶数和奇数两大类．另一方面，我们发现，除去1以外，有的数除了1和它本身以外，不能再被别的整数整除，如2，3，5，7，11，13，17，…这种数称作素数．有的数除了1和它本身以外，还能被别的数整除，这种数就叫作合数，如4，6，9，21，…就是合数．1这个数比较特殊，它既不算素数也不算合数．这样，所有正整数就又被分为1和素数、合数三类．正整数的这种分类要比它分为偶数和奇数两大类复杂多了．人们在很早以前就知道素数有无限多个，后来又知道素数的个数比合数要少得很多很多，但至今我们还没有一种能判断任意一个数是素数还是合数的简单可行的方法，甚至有的数我们根本不知道它是素数还是合数．现在我们所知道的最大的素数是$2^{21701}-1$．比它更大的素数虽然存在但目前我们还不知道．

合数与素数之间有什么关系呢？一个正整数如能被一个素数整除，那么这个素数就叫作是这个正整数的一个素因子。例如2是2的一个素因子，它也是10的素因子。显然一个素数就只有它本身一个素因子，而合数就可能有好几个素因子，如6就有2和3两个素因子，30就有2，3，5三个素因子，而4是有两个2作为它的素因子，叫做重因子。所以合数要比素数复杂多了，但合数又是它的所有素因子的乘积，如

$$4=2\times2,$$

$$30=2\times3\times5,$$

$$96=2\times2\times2\times2\times2\times3$$

等等。这样，一个合数的素因子的个数愈少愈简单，就愈近似地象一个素数。

容易看出在所有素数中只有一个2是偶数，其它全是奇数，叫做奇素数。

正整数可分为偶数和奇数，又可把它分为1，素数与合数，那么这两种分类之间究竟有什么联系呢？这是一个十分有趣的问题。

哥德巴赫猜想就是对这种联系的一种推测。

在科学研究中，人们在已有知识和实践的基础上往往小心地提出一些推测，以作进一步的研究，这些推测有的后来被证明是正确的，有的被证明是错误的，但也有的至今我们还不知道它是对是错，著名的哥德巴赫猜想就是这样一个至今还未证实的推测。

1742年6月7日德国数学家哥德巴赫在给当时的大数学家欧拉的信中，提出了这样两个推测：(1)每个不小于6

的偶数都是两个奇素数之和；(2)每个不小于 9 的奇数都是三个奇素数之和.这两个推测就是人们常说的哥德巴赫猜想.对许多偶数和奇数进行验算都表明这两个推测是正确的，例如

$$6 = 3 + 3,$$

$$24 = 11 + 13,$$

$$100 = 97 + 3,$$

以及

$$103 = 23 + 37 + 43$$

等等. 1742 年 6 月 30 日欧拉在复信中写道："任何大于 6 的偶数都是两个奇素数之和，虽然我还不能证明它，但我确信无疑认为这是完全正确的定理". 容易看出，由第一个推测可以推出第二个推测.由于欧拉是当时最伟大的数学家,因此他对这个推测的信心，便吸引了许多数学家的注意，都企图去证明它们.但是,当整个 19 世纪结束的时候,在研究这两个推测方面仍没有取得任何进展，甚至根本不知道应该如何下手. 1900 年德国大数学家希尔伯特在国际数学会的演说中，提出了具有重要意义的 23 个问题，这就是通常所说的希尔伯特问题. 哥德巴赫猜想被列为希尔伯特第 8 问题的一部分. 1912 年另一个德国数学家朗道在国际数学会的报告中说，即使要证明下面的较弱的命题："任何大于 4 的正整数，都能表示成 C 个素数之和"，也是现代数学家力所不能及的(这里 C 是某个常数). 1921 年英国数学家哈代曾说过哥德巴赫猜想的困难程度是可以和任何没有解决的数学问题相比的.

在本世纪 20 年代，英国数学家哈代与立脱伍特提出了

用所谓“圆法”来研究哥德巴赫猜想，第一次作出了意义极为重大的推进，并得到了一些初步成果。1937年苏联数学家依·维诺格拉陀夫在哈代—立脱伍特工作的基础上，用他自己创造的“三角和方法”首先基本上证明了第二个推测是正确的。确切地说，他证明了：每一个大奇数一定可以表示成三个奇素数之和。后来人们经过计算知道，这里所谓的“大奇数”是指一个差不多比10的400万次方即1后面加上400万个零这样一个数还要大的数，数字之大是无法用实际东西来比拟的。而目前已经知道的最大素数要比10的400万次方小得多，所以在这之间的许多奇数我们仍然不知道它们能否表示成三个奇素数之和。因而只能说是基本上解决了哥德巴赫的第二个推测。但这已是一个很重大的贡献了。

在依·维诺格拉陀夫的重要工作之后，我国数学家华罗庚在1938年证明了下面的重要定理：几乎全体偶数都能表示成两个素数之和。确切地说华罗庚证明了几乎全体偶数都能表示成 $p_1+p_2^k$ 的形式，这里 p_1，p_2 为素数，k 为任意给定的大于或等于1的自然数。这是华罗庚对第一个推测作出的重要贡献。

对于第一个推测，虽然现在已有人对 33×10^6 以下的每一个偶数进行验算都表明它是正确的，但要想证明它却是更为困难的了。很早以前，人们就退一步想，能否先来证明每一个大偶数都是二个素因子个数不太多的数之和，由此来找到一条通向解决第一个推测的道路。为了说起来简单起见，我们把“每一个大偶数可以表示为一个素因子个数不超过 a 个的数和一个素因子个数不超过 b 个的数之和”，这一命题叫作命题$(a+b)$。这样，哥德巴赫猜想基本上就是要证明命题

(1+1)是正确的。差不多在哈代—立脱伍特提出“圆法”的同时，1920年挪威数学家布朗在这方面迈出了具有重大意义的一步，在其开创性的论文中，第一个对古老的“筛法”作了重大的改进。他用“筛法”证明了每一个大偶数是二个素因子都不超过9个的数之和，即证明了命题(9+9)是正确的。其后许多数学家继续用布朗提出的方法，尽量减少其中每个数的素因子的个数。其中主要有：1924年拉得马哈证明了(7+7)；1932年爱斯特曼证明了(6+6)；1938年和1940年博赫石塔布又先后证明了(5+5)和(4+4)。后来，在1947年薛尔伯格对“筛法”作了进一步的改进，并在1950年宣布用他的方法可以证明(2+3)，但是始终没有给出他的证明。1956年我国数学家王元证明了(3+4)，同年阿·维诺格拉陀夫证明了(3+3)，直到1957年才由王元证明了命题(2+3)，这已经是愈来愈接近于命题(1+1)了。但以上所证明的结果都有一个共同的弱点，就是其中二个数没有一个可以肯定是为素数的。

早在1948年，匈牙利数学家兰恩易在其开创性的工作中，应用筛法和其它更为复杂的方法相结合，得到了一个有趣的结果，就是：每一个大偶数都是一个素数和一个素因子不超过C个的数之和，即证明了命题$(1+c)$。这是对研究哥德巴赫猜想的一个重大推进。但是他这里的C是一个没有计算出来的很大的未知常数。所以，这只是一个定性的结果。以后的十多年内在这方面也没有进一步的发展。1962年作者首先得到了C的定量估计，证明了$C=5$，即命题$(1+5)$成立。随后(同年)王元和作者证明了命题$(1+4)$，1963年巴帮也证明了该命题。1965年博赫石塔布、阿·维诺格拉陀夫和意

大利数学家朋比利又都证明了(1＋3)，特别是朋比利的工作，当时在国际数学界被认为是了不起的成就。

证明了命题(1＋3)后，我国数学家陈景润在1966年就已经宣布他证明了命题(1＋2)。但由于当时他没有发表详细的证明，所以在1973年以前的六年间，国际数学界仍然认为命题(1＋3)是最好的。因此，当陈景润于1973年，用他提出的方法发表了命题(1＋2)的全部证明后，在世界数学界引起了强烈的反响，这就是著名的“陈氏定理”，在陈景润的证明发表后的短短几年中，国际上又连续发表了五个简化证明，其中，丁夏畦、王元及作者都对“陈氏定理”给出了一个实质性的简化证明。

对于哥德巴赫猜想的研究还必须提及史尼尔曼的重要工作，在1930年史尼尔曼引入了关于自然数集合的“正密率”的概念，从而证明了每一整数可以表示成不超过C个素数之和。在史尼尔曼的工作发表后，曾有许多数学家利用了他的方法，并结合“筛法”得到了一系列的结果。若我们用S表示最小的整数，使每一充分大的整数都能表示成不超过S个素数之和，则：用史尼尔曼的方法可以得到S的明确上界。他的方法可以算出$S\leqslant 8\times 10^6$。罗曼诺夫以后又证明了$S\leqslant 2208$。沿着这一方向还有许多数学家作了更进一步的改进。1950年夏皮洛与瓦格利用薛尔伯格的筛法证明了$S\leqslant 20$，1956年我国数学家尹文霖利用渐近密率的方法又将20改进成18，而最好的结果是最近沃恩证明的$S\leqslant 6$*。

---

* 用前面提到的维诺格拉陀夫将大奇数表成三个素数的定理可以推出$S\leqslant 4$。但维氏所用的方法是相当高级的，而这里的方法却较为“初等些”。

哥德巴赫猜想从提出到今天已经快要过去二个半世纪了，虽有很多进展，但还未完全解决。研究哥德巴赫猜想的历史，生动地说明了攀登科学高峰的征途是艰难、漫长而又曲折的，经过许多卓越数学家的辛勤劳动才取得了今天这样的成就。解放后的新中国，培养了一批年轻的数学工作者，他们在华罗庚教授与闵嗣鹤教授的指导帮助下，曾对哥德巴赫猜想等数论专题方面的研究作出了重要的贡献。

但是应该看到，二百多年来，虽然在研究哥德巴赫猜想中取得了这样重大的成就，要从(1＋2)到完全解决哥德巴赫猜想还有十分漫长的路程。或许，我们可以说，为了完全解决哥德巴赫猜想（不管是肯定的，还是否定的）所需克服的困难可能比至今克服的困难更为巨大。因为依作者看来，不仅现有的方法不适用于来研究解决(1＋1)，而且到目前为止还看不到可以沿着什么途径，利用什么方法来解决它。

第二章　整数的基本性质

本章主要介绍一些整数的基本性质。

2·1　整数的可除性

整数是指

$$\cdots,\ -2,\ -1,\ 0,\ 1,\ 2,\ \cdots$$

显然，二整数之和、差、积仍为整数，但是，用一不等于零的整数去除另一个整数，所得的商却不一定是整数。我们用$[\alpha]$来表示不超过α的最大整数，例如

$$[4]=4,\ [3.1]=3,\ [-2.4]=-3,\ [\pi]=3.$$

下面的不等式是显然成立的：

$$[\alpha]\leqslant\alpha<[\alpha]+1$$

现在取α为有理数$\frac{a}{b}(b>0)$，则由上面的不等式可得到

$$0\leqslant\frac{a}{b}-\left[\frac{a}{b}\right]<1,$$

亦即

$$0\leqslant a-b\left[\frac{a}{b}\right]<b.$$

由此立得

$$a=\left[\frac{a}{b}\right]b+r,\quad 0\leqslant r<b.$$

因此，我们可以得到下面的定理：

定理 2·1 任给二整数 a，$b>0$，必有二整数 q 及 r 存在，使得

$$a=qb+r, \quad 0\leqslant r<b. \tag{2.1}$$

且 q 及 r 是唯一存在的。

证：我们只要来证明唯一性就够了。

若还存在 q_1，r_1 使得

$$a=q_1b+r_1, \quad 0\leqslant r_1<b$$

则有

$$b(q-q_1)=r-r_1.$$

由于 r 及 r_1 为不超过 b 的正数，所以 $|r-r_1|$ 不可能超过 b，但由上式得到

$$b|q-q_1|=|r-r_1|$$

若 $q\neq q_1$，则必有 $|r-r_1|>b$，而这是不可能的。所以必有 $q=q_1$，从而推出 $r=r_1$，定理证毕。

定理 2·1 是一条基本定理，整数的很多基本性质都可以从它引出。这里 q 称为不完全商数，r 称为余数。

当 $r=0$ 时的情形是值得注意的；此时公式 (2.1) 变成 $a=qb$ 或 $\frac{a}{b}=q$。这种情形我们就说，a 被 b 除尽，b 是 a 的因数；a 是 b 的倍数。我们用 $b|a$ 来表示 b 除得尽 a。

2·2 最大公因数与最小公倍数

设 a，b 是两个整数。若整数 d 是它们之中每一个的因数，那末 d 就叫作 a，b 的一个公因数。a，b 的所有公因数

中最大的一个叫作 a，b 的最大公因数，记作 (a, b)。若 $(a,b)=1$，则我们说 a，b 是互素的。不难看出，a,b 的公因数与 $|a|$，$|b|$ 的公因数相同，因而有

$$(a, b)=(|a|, |b|)。 \tag{2.2}$$

所以我们讨论最大公因数不妨就非负整数的情形去讨论。

若 a，b，c 是三个不全为零的整数，且有

$$a=bq+c, \tag{2.3}$$

则容易证明必有

$$(a, b)=(b, c)。 \tag{2.4}$$

我们现在要利用上面的关系来给出一个求最大公因数的方法——辗转相除法。

设 a，b 是任意两个正整数，反复利用定理 2·1，可以得到

$$\begin{aligned}
&a=bq_1+r_1, && 0<r_1<b,\\
&b=r_1q_2+r_2, && 0<r_2<r_1,\\
&r_1=r_2q_3+r_3, && 0<r_3<r_2,\\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots && \qquad (2.5)\\
&r_{n-2}=r_{n-1}q_n+r_n, && 0<r_n<r_{n-1},\\
&r_{n-1}=r_nq_{n+1}+r_{n+1}, && r_{n+1}=0。
\end{aligned}$$

因为每进行一次除法，余数就至少减一，而 b 是有限的，所以我们至多进行 b 次，总可以得到一个余数是零的等式，即 $r_{n+1}=0$。上面的方法我们叫作辗转相除法，也叫长除法。是我国古代数学家创造的，但在一般书中常把它叫欧几里得除法。下面给出辗转相除法的一个应用。

定理 2·2 设 a，b 是任意两个正整数，则有

$$(a, b)=r_n$$

证：事实上，利用(2.4)及(2.5)式便可以得到：

$$r_n=(0,\ r_n)=(r_{n+1},\ r_n)=(r_n,\ r_{n-1})=\cdots$$
$$=(r_1,\ b)=(a,\ b).$$

定理 2·2 实际上给出了一个求最大公因数的方法．当 a，b 中有一个为零时，$(a,\ b)$就等于不为零的数的绝对值，若 a，b 都不为零时，就可利用上面的方法求出其最大公因数．

例 2·1　求$(-123,\ 18)$.

我们有

$$(-123,\ 18)=(123,\ 18)$$
$$123=6\times 18+15,$$
$$18=1\times 15+3,$$
$$15=5\times 3.$$

所以

$$(-123,\ 18)=3.$$

下面的定理给出了最大公因数的两个重要性质：

定理 2·3　设 a，b 是两个正整数，则

(1)

$$(am,\ bm)=(a,\ b)m, \tag{2.6}$$

这里 m 为任意正整数.

(2) 若 d 是 a，b 的任一公因数，则

$$\left(\frac{a}{d},\ \frac{b}{d}\right)=\frac{(a,\ b)}{d}. \tag{2.7}$$

特别有

$$\left(\frac{a}{(a,\ b)},\ \frac{b}{(a,\ b)}\right)=1. \tag{2.8}$$

证： 由辗转相除法得到

$$am=(bm)q_1+r_1m, \quad 0<r_1m<bm,$$

$$bm=(r_1m)q_2+r_2m, \quad 0<r_2m<r_1m,$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$r_{n-1}m=(r_nm)q_{n+1}.$$

由定理2·2，得

$$(am,\ bm)=r_nm=(a,\ b)m.$$

因而(1)得证.

利用(1)的结论立即推出

$$\left(\frac{a}{d},\ \frac{b}{d}\right)=\frac{(a,\ b)}{d}.$$

取 $d=(a,\ b)$，即得(2.8)．定理证毕.

下面来引进最小公倍数的概念．设 a，b 为两个整数，若 d 是这两个数的倍数，则 d 就叫作 a，b 的公倍数．在 a，b 的一切公倍数中的最小正数叫作 a，b 的最小公倍数，记作 $[a,\ b]$.

我们首先来证明下面的事实：

若 m_1 为 a，b 的一个公倍数，则必有

$$[a,\ b]\mid m_1. \tag{2.9}$$

我们令

$$m=[a,\ b]$$

因为 $m<m_1$，所以由定理2·1知

$$m_1=qm+r; \quad 0\leqslant r<m.$$

由假设知，m，m_1 都是 a，b 的公倍数，故

$$r=m_1-qm$$

亦为 a，b 的公倍数．但 $r<m$，而 m 是最小公倍数，故必有