数学名著译丛

博大精深的素数

〔加拿大〕P. 里本伯姆 著
孙淑玲 冯克勤 译

科学出版社
www.sciencep.com

数学名著译丛

博大精深的素数

〔加拿大〕P. 里本伯姆 著

孙淑玲 冯克勤 译

科学出版社

北京

图字：01-2006-2858 号

内 容 简 介

本书介绍了从欧几里得、费马、欧拉、高斯以来 2000 多年中素数研究的重要成果、问题、思想和方法，包括素数有多少、如何识别素数、是否有定义素数的函数等一系列具有重要理论意义和应用背景的问题，并介绍了相关问题至 2003 年的最新记录.

本书内容全面、新颖，可供大学数学系高年级学生、研究生、教师以及从事数学、信息科学等工作的科研人员阅读参考.

图书在版编目(CIP)数据

博大精深的素数/(加拿大)P. 里本伯姆著；孙淑玲，冯克勤 译.
—北京：科学出版社，2007
(数学名著译丛)
ISBN 978-7-03-017370-6

I. 博… II. ①P… ②孙… ③冯… III. 素数-普及读物
IV. O156.2-49

中国版本图书馆 CIP 数据核字(2006)第 058449 号

责任编辑：吕 虹 张 扬 张启男 杨 然/责任校对：张小霞
责任印制：安春生/封面设计：王 浩

科学出版社 出版
北京东黄城根北街 16 号
邮政编码：100717
http://www.sciencep.com

新蕾印刷厂 印刷

科学出版社编务公司排版制作
科学出版社发行 各地新华书店经销
*

2007 年 1 月第 一 版 开本：(850×1168) 1/32
2007 年 1 月第一次印刷 印张：11 1/4
印数：1—3 000 字数：288 000

定价：38.00 元

(如有印装质量问题，我社负责调换〈环伟〉)

前　言

《吉尼斯记录大全》一书已家喻户晓. 人们在喝具有吉尼斯商标烈性啤酒时进行友好的争辩, 此书成为解决争端最权威的信息源泉, 它成功地记录了各种英勇事迹、超常行为、耐力表演等. 而这些记录反过来又影响和激发了更多人做同样的尝试. 于是人们会看到, 双人舞无休止地进行、有人和蛇一起呆在棺材里. 这些活动周而复始地举行, 只是为了在这本记录琐事的圣经中留下自己的名字. 书中也有体育记录以及身高体重和生育等方面的超常事实等.

在这本书中很少记录科学领域的事情. 事实上, 科学家尤其是数学家在酒吧里喝红酒或啤酒时也很喜欢聊天. 在喝了一阵之后, 也会对诸如关于新发现的某种数等各样最新记录打赌.

老实说, 假如我在《辉格标准报》中能够读到, 人们在公众场合的吵架是源于对目前已知的最大孪生素数对的激烈争辩, 我会觉得这种吵架更文明一些.

但是, 不是每个人都认为人们之间的争斗是所希望的, 即使这种争斗有很重要的理由. 所以, 我想揭示某些记录. 任何人若是知道更好的记录, 请把新的信息告诉我.

我只讨论素数: 它们是一些自然数 2,3,5,7,11,$\cdots$ 它们不会被任何比它小的自然数 (除了 1 之外) 除尽. 若自然数不是 1 也不是素数, 则叫作合成数.

素数是重要的, 因为算术基本定理说, 每个大于 1 的自然数均是素数的乘积, 并且这种分解本质上是唯一的.

“哪个素数是特别的?” 不用说, 这是一个很容易回答的问题: 是素数 2, 因为它是偶素数!

遇到素数的机会 (例如 1093 和 608981813029) 并不大，它们有各种有趣的性质. 素数彼此很像表姐妹，她们是同一家族的成员，彼此长得很像，但又不完全一样.

在讲述关于素数的各种记录的时候，我首先遇到的问题是如何组织这些材料. 也就是说，对于素数理论的研究和发展如何分成几条主线.

一般来说，在研究某个数集 (我们这里是素数集合) 的时候，会问到下列一些问题：该集合有多少数？如何决定任意一个数是否属于这个数集？如何描述这些数？这种数在绝对值很大时或在小区间中分布如何？然后便集中注意这种数的各种类型，同时对这些数做各种试验，于是像其他科学领域中那样提出一些猜测.

按这种方式，我们把素数问题分成以下几个专题：

(1) 素数有多少？

(2) 如何识别一个自然数是否为素数？

(3) 是否存在定义素数的一些函数？

(4) 素数的分布如何？

(5) 哪些素数的特殊性质需要考虑？

(6) 关于素数的实验和概率统计结果.

在讨论这些问题时我们将提供素数的有关记录.

数 学 符 号

符号	含义
$m \mid n$	整数 m 整除整数 n
$m \nmid n$	整数 m 不能整除整数 n
$p^e \parallel n$	p 是素数， $p^e \mid n$ 但 $p^{e+1} \nmid n$
$\gcd(m,n)$	整数 m,n 的最大公因子
$lcm(m,n)$	整数 m,n 的最小公倍数
$\log(x)$	实数 $x>0$ 的自然对数
$\mathbb{Z}$	整数环
$\mathbb{Q}$	有理数域
$\mathbb{R}$	实数域
$\mathbb{C}$	复数域

下面列出在书中出现的符号

符号	含义
p_n	第 n 个素数
$p\#$	小于 p 的所有素数的乘积，或叫 p 的素连乘
F_n	第 n 个费马数， $F_n = 2^{2^n}+1$
$[x]$	x 的整数部分，即满足 $[x] \leqslant x \leqslant [x]+1$ 的唯一整数 $[x]$
g_p	模 p 的最小原根
$\varphi(n)$	欧拉函数
$\lambda(n)$	Carmichael 函数
$\omega(n)$	n 的不同素因子个数
$L(x)$	$n \leqslant x$ 且 $\varphi(n)$ 整除 $n-1$ 的合成数 n 的个数

符号	含义
$V_\psi(m)$	$\#\{n \geqslant 1 \mid \varphi(n)=m\}$
t_n^*	a^n-b^n 的主要部分
$k(m)$	m 的无平方因子
$P[m]$	m 的最大素因子
S_r	至多有 $r\log\log n$ 个不同素因子的整数 n 全体
$\left(\frac{a}{p}\right)$ 或 $(a \mid p)$	Legendre 符号
$\left(\frac{a}{b}\right)$ 或 $(a \mid b)$	Jacobi 符号
$U_n=U_n(P,Q)$	参数为 (P,Q)Lucas 序列的第 n 项
$V_n=V_n(P,Q)$	参数为 (P,Q)Lucas 序列的第 n 项
$\rho(n)=\rho(n,U)$	n 能整除 U_r 的最小 r
$\psi(p)$	$=p-(D \mid p)$
$\left(\frac{\alpha,\beta}{p}\right)$	与 X^2-PX+Q 的两个根 α,β 有关的符号
$\psi_{\alpha,\beta}(p)$	$=p-\left(\frac{\alpha,\beta}{p}\right)$ 其中 p 是奇素数
$\psi_{\alpha,\beta}(p^e)$	$=p^{e-1}\psi_{\alpha,\beta}(p)$ 其中 p 是奇素数
$\lambda_{\alpha,\beta}\left(\prod p^e\right)$	$lcm\{\psi_{\alpha,\beta}(p^e)\}$
$\mathcal{P}(U)$	整除某项 $U_n\neq 0$ 的素数全体
$\mathcal{P}(V)$	整除某项 $V_n\neq 0$ 的素数全体
U_n^*	U_n 的本原部分
$\psi_D\left(\prod_{i=1}^s p_i^{e_i}\right)$	$=\frac{1}{2^{s-1}}\prod_{i=1}^s\left(p_i^{e_i-1}-\left(p_i-\left(\frac{D}{p_i}\right)\right)\right)$
Pn	有 n 位数字的素数
Cn	有 n 位数字的合成数
M_q	$=2^q-1$， Mersenne 数

符号	含义
$\sigma(n)$	n 的因子之和
$\tau(n)$	n 的因子个数
$H(n)$	n 的因子的调和平均
$V(x)$	x 以内完全数的个数
$s(n)$	n 的真因子之和
psp	以 2 为基的拟素数
$\mathrm{psp}(a)$	以 a 为基的拟素数
$B_{\mathrm{psp}}(n)$	$\#\{a\|1 < a \leqslant n-1, \gcd(a,n)=1, n$为 $\mathrm{psp}(a)\}$
$\mathrm{epsp}(a)$	以 a 为基的欧拉拟素数
$B_{\mathrm{epsp}}(n)$	$\#\{a\|1 < a \leqslant n-1, \gcd(a,n)=1, n$为 $\mathrm{epsp}(a)\}$
$\mathrm{spsp}(a)$	以 a 为基的强欧拉拟素数
$B_{\mathrm{spsp}}(n)$	$\#\{a\|1 < a \leqslant n-1, \gcd(a,n)=1, n$为 $\mathrm{spsp}(a)\}$
$M_3(m)$	$=(6m+1)(12m+1)(18m+1)$
$M_k(m)$	$=(6m+1)(12m+1)\prod_{i=1}^{k-2}(9\times 2^i m+1)$
C_k	如果 $1 < a \leqslant n-1, \gcd(a,n)=1$，则 $a^{n-k} \equiv 1(mod\ n)$. 满足上述条件且大于 k 的合成数 n 全体 (当 $k>1$ 时为 Knödel 数)
$\mathrm{lpsp}(P,Q)$	具有参数 (P,Q) 的 Lucas 拟素数
$B_{\mathrm{lpsp}}(n,D)$	$\#\{1 < P \leqslant n$存在Q, 使得$D \equiv P^2-4Q\ (mod\ n)$为 $\mathrm{lpsp}(P,Q)\}$
$elpsp(P,Q)$	具有参数 (P,Q) 的 Euler-Lucas 拟素数
$slpsp(P,Q)$	具有参数 (P,Q) 的强 Lucas 拟素数
$\pi(x)$	小于 x 的素数个数
$\mu(x)$	Möbius 函数
Δ	与 $d \neq 0,1$ 结合的基本判别式

符号	含义
$\mathbb{Q}(\sqrt{d})$	$=\mathbb{Q}(\sqrt{\Delta})$，二次域
Cl_d或Cl_Δ	$\mathbb{Q}(\sqrt{d})$ 的类群
h_d或h_Δ	$\mathbb{Q}(\sqrt{d})$ 的类数
e_d	Cl_d 类群的指数
$\pi^*_{f(X)}(N)$	$\#\{n \mid 0 \leqslant n \leqslant N, \lvert f(n)\rvert$是素数$\}$
$P_0[m]$	$m>1$ 的最小素因子
$P_0[f(X)]$	$\min\{P_0[f(X)] \mid k=0,1,2,\cdots\}$
$f(x)\sim h(x)$	f,h 渐近相等
$f(x)=g(x)+O(h(x))$	差 $f(x)-g(x)$ 以 $h(x)$ 的常数倍数为上界
$f(x)=g(x)+o(h(x))$	差 $f(x)-g(x)$ 与 $h(x)$ 比较可忽略不计
$\zeta(s)$	黎曼 Zeta 函数
B_k	Bernoulli 数
$S_k(n)$	$=\sum_{j=1}^{n} j^k$
$B_k(X)$	Bernoulli 多项式
$Li(x)$	对数积分
$\theta(x)$	$=\sum_{p\leqslant x}\log p$, Tschebycheff 函数
$Re(s)$	s 的实数部分
$\Gamma(s)$	Gamma 函数
γ	欧拉常数
$J(x)$	加权的素数幂计算函数
$R(x)$	黎曼函数
$\Lambda(x)$	van Mangoldt 函数
$\varphi(x)$	van Mangoldt 函数的求和函数
$M(x)$	Mertens 函数
$\varphi(x,m)$	$\#\{a \mid 1 \leqslant a \leqslant x, a$不是$1,2,\cdots,p_m$倍数$\}$

符号	含义
ρ_n	zeta 函数在临界区域的上半平面部分的第 n 个非平凡零点
$N(T)$	$\#\{\rho=\sigma+it \mid 0\leqslant\sigma\leqslant 1, \varsigma(\rho)=0, 0<t\leqslant T\}$
d_n	$=p_{n+1}-p_n$
$g(p)$	大于 p 的连续合成数的个数
G	$=\{m \mid$ 对某个$p>2, m=g(p)\}$
$p[m]$	使得 $g(p)=m$ 的最小素数 p
$\log_2 x$	$\log\log x$
$\log_3 x$	$\log\log\log x$
$\log_4 x$	$\log\log\log\log x$
B	Brun 常数
$\pi_2(x)$	$\#\{$素数$p \mid p+2\leqslant x$且$p+2$也是素数$\}$
C_2	$=\prod_{p>2}\left(1-\frac{1}{(p-1)^2}\right)$，李生素数常数
$\pi_{2k}(x)$	$\#\{n\geqslant 1 \mid p_n\leqslant\ and\ p_{n+1}-p_n=2k\}$
$\pi_{2,6}(x)$	$\#\{$素数$p \mid p\leqslant x$且$p+2, p+6$也是素数$\}$
$\pi_{4,6}(x)$	$\#\{$素数$p \mid p\leqslant x$且$p+4, p+6$也是素数$\}$
$\pi_{2,6,8}(x)$	$\#\{$素数$p \mid p\leqslant x$且$p+2, p+6, p+8$ 也是素数 $\}$
$B_{2.6}$	$=\sum\left(\frac{1}{p}+\frac{1}{p+2}+\frac{1}{p+6}\right)$ 在所有素数三元组 $(p, p+2, p+6)$ 上求和
$B_{4.6}$	$=\sum\left(\frac{1}{p}+\frac{1}{p+4}+\frac{1}{p+6}\right)$ 在所有素数三元组 $(p, p+4, p+6)$ 上求和
$B_{2,6,8}$	$=\sum\left(\frac{1}{p}+\frac{1}{p+2}+\frac{1}{p+6}+\frac{1}{p+8}\right)$ 在所有素数四元组 $(p, p+2, p+6, p+8)$ 上求和
$\rho^*(x)$	$=k$表示存在允许的 $(k-1)-$ 数组 $b_1, b_2, \cdots, b_{k-1}$ 使得 $b_{k-1}<x$ 但是不存在多于 $k-1$ 个分量的

符号	含义
	这种数组
$\rho(x)$	$=\limsup_{y\to\infty}(\pi(x+y)-\pi(y))$
$\pi_{d,a}(x)$	$\#\{$素数$p \mid p\leqslant x, p\equiv a(mod\ d)\}$
$p(d,a)$	在算术级数 $\{a+kd \mid k\geqslant 0\}$ 中最小的素数
$p(d)$	$=\max\{p(d,a) \mid 1\leqslant a<d, \gcd(a,d)=1\}$
L	Linnik 常数
P_k	k 殆素数集合
S, S_0	Schnirelmann 常数
$r_2(2n)$	$2n$ 表示成两个素数和的方法数
$G'(n)$	$\#\{2n \mid 2n\leqslant x, 2n$不是两个素数和$\}$
$(psp)_n$	第 n 个拟素数
$P\pi(x)$	小于等于 x 的基为 2 的拟素数的个数
$P\pi_a(x)$	小于等于 x 的基为 a 的拟素数的个数
$EP\pi(x)$	小于等于 x 的基为 2 的欧拉拟素数的个数
$EP\pi_a(x)$	小于等于 x 的基为 a 的欧拉拟素数的个数
$SP\pi(x)$	小于等于 x 的基为 2 的强拟素数的个数
$SP\pi_a(x)$	小于等于 x 的基为 a 的强拟素数的个数
$l(x)$	$=\mathrm{e}^{\log x\log\log\log x/\log\log x}$
$psp(d,a)$	$\gcd(a,d)=1$，在算术级数 $\{a+kd \mid k\geqslant 0\}$ 中最小的拟素数
$CN(x)$	$\#\{n \mid 1\leqslant n\leqslant x, n$是 Carmichael 数$\}$
$L\pi(x)$	具有 (P,Q) 参数且小于等于 x 的 Lucas 拟素数个数
$SL\pi(x)$	具有 (P,Q) 参数且小于等于 x 的 Lucas 强拟素数个数

符号	含义
ς_p	$=\cos(2\pi/p)+\mathrm{i}\sin(2\pi/p)$
$h(p)$	第 p 个分圆域的类数
$\pi_{reg}(x)$	$p\leqslant x$ 的正规素数的个数
$\pi_{ir}(x)$	$p\leqslant x$ 的非正规素数的个数
$ii(p)$	p 的不正规指数
$\pi_{iis}(x)$	满足 $p\leqslant x, ii(p)=s$ 的素数 p 的个数
$S_{d,a}(x)$	$\#\{p$是素数 $\mid p\leqslant x, dp+a$是素数$\}$
$q_p(a)$	$=\frac{a^{p-1}-1}{p}$， p 的基为 a 的费马商
$W(p)$	$=\frac{(p-1)!+1}{p}$， Wilson 商
Rn	$\frac{10^n-1}{9}$
Cn	$=n\times 2^n+1$， Cullen 数
$C\pi(x)$	$\#\{n\mid C_n\leqslant x$且C_n是素数$\}$
Wn	$=n\times 2^n-1$， Woodall 数或第二类 Cullen 数
$\mathcal{P}(T)$	整除序列 $T=(T_n)_{n\geqslant 0}$ 中某项的素数全体
$\pi_H(x)$	$\#\{p\in P(H)\mid p\leqslant x\}$
S_{2n+1}	NSW 数
$\pi_{f(X)}(x)$	$\#\{n\geqslant 1\mid \lvert f(n)\rvert\leqslant x$且$\lvert f(n)\rvert$是素数$\}$
$p(f)$	使得 $\lvert f(m)\rvert$ 是素数的最小整数 $m\geqslant 1$
$\pi_{X.X+2k}(x)$	$\#\{$素数$p\mid p+2k$是素数且$p+2k\leqslant x\}$
$\pi_{X^2+1}(x)$	$\#\{$素数$p\mid$ 要求$p=m^2+1, p\leqslant x\}$
$\pi_{aX^2+bX+c}(x)$	$\#\{$素数$p\mid$ 要求$p=am^2+bm+c, p\leqslant x\}$

目　录

第一章　素数有多少？

这个问题的答案是下列基本定理：

素数有无穷多个.

我将给出这个定理的七个证明 (再加上这些证明的四个变种), 这些证明均由著名数学家给出，其中有些数学家已被人遗忘. 其中一些证明引发出有趣的新发展，另一些证明也很聪明和巧妙. 当然还有更多的关于素数无穷的证明 (当然没有无穷多个证明).

1.1　欧几里得 (Euclid) 的证明

假设 $p_1 = 2 < p_2 = 3 < \cdots < p_r$ 是全部素数，令 $P = p_1p_2\cdots p_r+1$, 并且 p 为除尽 P 的一个素数, 则 p 不能是 $p_1, p_2, \cdots, p_r$ 当中的任何一个. 因为否则，将除尽差数 $P - p_1p_2\cdots p_r = 1$, 而这是不可能的. 所以 p 又是一个新的素数，从而 $p_1, p_2, \cdots, p_r$ 不能为全部素数. □

我们把素数按递增的顺序写成一个序列

$$p_1 = 2,\ p_2 = 3,\ p_3 = 5,\ p_4 = 7,\ \cdots,\ p_n,\ \cdots$$

1878 年，库默尔 (Kummer) 给出欧几里得证明的一个巧妙的新形式.

库默尔的证明　假设只有有限多个素数 $p_1 < p_2 < \cdots < p_r$. 令 $N = p_1p_2\cdots p_r > 2$, 则整数 $N - 1$ 为一些素数的乘积，从而必有某个 p_i 为 N 的素因子，于是 p_i 除尽 $N - (N - 1) = 1$, 这又推