数学名著译丛

数论中未解决的问题

（第二版）

〔加〕R．K．盖伊　著

张明尧　译

北　京

内 容 简 介

本书分 6 个部分，介绍了数论中大量未解决的问题（个别问题现在已解决了），其中包括：素数，整除性，堆垒数论，不定方程，整数序列及其他问题．目的是向初次涉及研究工作的人以及有一定工作经历，但缺乏合适的数学问题的人，提供一批容易理解（即便并不容易解决）的问题．

本书可供科研人员，大学数学系师生，数学爱好者阅读．

图字：01-2001-0353 号
图书在版编目（CIP）数据

数论中未解决的问题（第二版）/（加）盖伊（Guy，R.K.）著；张明尧译．—北京：科学出版社，2002
（数学名著译丛）
ISBN 7-03-010310-6

Ⅰ.数… Ⅱ.①盖…②张… Ⅲ.数论-数学问题-研究
Ⅳ.O156

中国版本图书馆 CIP 数据核字（2002）第 018818 号

责任编辑：毕 颖/责任校对：钟 洋
责任印制：安春生/封面设计：王 浩

科学出版社发行 各地新华书店经销

*

2003 年 1 月第 一 版 开本：850×1168 1/32
2003 年 1 月第一次印刷 印张：11 3/8
印数：1—3 000 字数：288 000

定价：23.00 元

（如有印装质量问题，我社负责调换〈环伟〉）

中文版前言

中国人和世界上其他文明古国的人民一样，很早就对数学的发展做出了贡献，他们对数学做出的贡献要比世界上多数国家更为久远．然而东西方的交流一度不是十分通畅．举例来说，直到最近我们才知道，Catalan 数不仅在 Catalan 之前 100 多年就被 Euler，Fuss 以及 Segner 等人研究过，而且在他们之前就被中国数学家明安图研究过（译者注：明安图（？～1765），我国清代数学家、天文学家，字静庵，蒙族人，曾任钦天监监正，主要著作有《割圆密率捷法》四卷等）．

中国人对数学的贡献在数论中表现得尤为突出．在现代中国有华罗庚、闵嗣鹤以及他们的学生，尤其是陈景润、王元和潘承洞，现在又有了第三代数学家．他们在经典数论的许多问题，诸如 Goldbach 猜想、Gauss 整点问题、Tarry 问题、Waring 问题以及有关素数分布等问题的研究中都取得了重要的成果，并且正在做着重要的贡献．

在这里我要感谢译者张明尧在将我这本激励了众多西方读者的数论问题集介绍给中国读者时所做的工作．如果书中任何问题有了新的进展，请读者不吝赐教，以便这些新的进展可以写进本书未来的新版之中．

R．K 盖伊
2002 年 3 月
卡尔加里大学
阿尔伯塔，加拿大

第二版前言

Erdös 回忆起 1912 年在剑桥举行的国际数学家大会上，Landau 曾就素数和提及的在当时的学术条件下无法解决的 4 个问题（见下面的 A1，A5，C1）作过一个讲话. 他说这些问题现在仍然无法解决. 另一方面，自本书第一版问世以来，已有了一些惊人的进展. Fermat 大定理（有个小的漏洞预期可得以弥补）、Mordell 猜想、Carmichael 数的无穷性等一批问题已经获得解决.（Fermat 大定理证明中的漏洞已由 Andrew Wiles 等人完全解决——译者注）

本书永远是落后于时代的，其差距虽然并不总是像在第一版的问题 D1 中一个命题那样有 1700 年之久，但至少在昨天的条目和读者阅读首批上市的新书之间要相差几个月的时间. 为使读者与本书第一版容易进行比较，每节的编号保持不变. 大部或全部获得解决的问题有 B47，D2，D6，D8，D16，D26，D27，D28，E15，F15，F17 及 F28. 在某些情形附加了一些有关的开放问题；而在另一些情形，涉及到的一些没有解决的问题不是作为问题，而是作为练习放了进来.

现将作者的两个特别喜欢使用的符号说明如下：其一是用 & 表示合作的工作，以消除任何可能的含混不清之处. 例如“……得自 Gauss 的工作以及 Erdös 和（&）Guy 的工作”；其二是从匈牙利人那儿借用的符号¿……?，它表示一个猜测或假想的命题. 一本初等微积分教材的作者，他有良好的意图却未得到好的建议. 如果他能在书中用此符号，当可避免某些精神上的痛楚. 有一个学生在求乘积函数的导数时发生了困难，在我感到失望之时，我想到要求看一看那个学生的教科书. 我看到他在书上用醒目的记号标出一个公式：乘积的导数等于导数的乘积. 可是

他却没有注意到书上说的是“为什么……不是正确的答案?”

以前提到的《几何中未解决的问题》一书现已出版，而且是作为重印本或作为第二版发行.

由本书可以清楚地看到，有多少人接受了我的邀请，利用它来交换有关问题的信息；而我又是如何从与读者的通信中获益匪浅的. 尽管我已经将致谢的名单大大扩大了，但这份名单仍不完全. 不过我至少应该感谢 Harvey Abbott，Arthur Baragar，Paul Bateman，T. G. Berry，Andrew Bremner，John Brillhart，R. H. Buchholz，Duncan Buell，Joe Buhler，Mitchell Dickerman，Hugh Edgar，Paul Erdös，Steven Finch，Aviezri Fraenkel，David Gale，Sol Golomb，Ron Graham，Sid Graham，Andrew Granville，Heiko Harborth，Roger Heath-Brown，Martin Helm，Gerd Hofmeister，Wilfrid Keller，Arnfried Kemnitz，Jeffrey Lagarias，Jean Lagrange，John Leech，Dick Lehmer，Emma Lehmer，Hendrik Lenstra，Hugh Montgomery，Peter Montgomery，Shigeru Nakamura，Richard Nowakowski，Andrew Odlyzko，Richard Pinch，Carl Pomerance，Aaron Potler，Herman te Riele，Raphael Robinson，Øystein Rødseth，K. R. S. Sastry，Andrzej Schinzel，Reese Scott，John Selfridge，Ernst Selmer，Jeffrey Shallit，Neil Sloane，Stephane Vandemergel，Benne de Weger，Hugh Williams，Jeff Young 和 Don Zagier. 没有 John Leech 完美的校对，没有他广博的文献知识以及明晰的数学思想和创见，本书将会大为逊色.

作者还要感谢 Andy Guy 为本书创建的电子体系，它使得作者和出版社两方面的工作都轻松了许多. 我们还要感谢加拿大国立科学和工程研究理事会对本书和作者的许多其他项目始终如一的支持.

R. K. 盖伊

1994. 1. 8 于卡尔加里

第一版前言

在许多外行人看来，数学家好像就是解题之人，也就是俗话说的“解算术难题的人”. 即便在数学界内部，数学家们也把自己分成理论研究者和问题求解者两类人. 数学能保持其生命力，比上述两类人的工作更为重要的是依赖于来自数学本身以及来自日益增多的应用领域的一系列问题. 数学常受惠于提出问题者比受惠于回答问题者要更多. 求解一个问题或许会抑制人们对该领域的兴趣. 而“Fermat 大定理”正因为还不是一个定理，它产生了大量“好的”数学——至于数学的好坏，是由它的美、深度及可应用性来加以判别的.

提出好的未解决问题是一门艰难的艺术. 在平庸无聊的问题和几乎无望求解的问题之间求得平衡是困难而微妙的. 有许多易于表述的问题，专家告诉我们，这些问题到下一代也不太可能获得解决. 即使我们不能活着看到 Riemann 猜想、Goldbach 猜想、孪生素数猜想、Mersenne 素数猜想或者奇完全数猜想的解决，然而我们却看到了四色猜想的解决. 从另一方面来说，“未解决的”问题未必就是根本不可解的，或许可能比我们一开始所想的要容易得多.

在匈牙利数学家 P. Erdös 所做出的许多贡献中，并非最不起眼的是他源源不断提出来的一系列出色的问题. 好像这些问题还不够刺激似的，他还对许多问题的第一个解决者予以悬赏奖励，同时对问题的难度给出他自己的估计. 为此他已付出了许多钱，奖金从 1 美元到 1000 美元不等.

本书的目的之一是向初次涉及研究工作的人以及那些虽然更为成熟、但缺乏合适的数学问题刺激的人提供一批容易理解（即便并不容易解决）的问题. 他们可以在不同的深度上考虑这些问

题，有时能获得部分进展，从而逐渐赢得兴趣、信心和恒心，这些都是研究工作获得成功的要素.

本书还有更为广泛的目标. 对那些水平高低各不相同的学习数学的学生和数学教师来说，虽然他们没有能力做研究工作，或许对此也并无希冀或雄心，然而重要的是有大批他们能够理解的未解决的问题，其中有些问题会在他们的一生中得到解决. 有许多业余数学爱好者被吸引过来，有许多成功的研究工作者一开始就是通过对 Euclid 几何、数论中的问题（最近是对组合和图论中的问题）加以研究而赢得信心的. 在这些领域中他们有可能不需要在理论上有很深的预备知识就看得懂问题，甚至能用式子表达问题并得到初步的结果.

本书的思想可追溯到大约 20 年前，那时我被流传的由已故的 Leo Moser 及其合作者 Hallard Croft 所写的问题册以及 Erdös 的文章深深吸引. Croft 同意让我帮助他把他的问题册扩大写成一本书，而 Erdös 则不断地鼓励、督促我们. 过了一些时候，数论这一章已经膨胀成了一部系列丛书中的一卷，这一系列丛书还将包括几何卷、凸性和分析卷，它们由 Hallard Croft 撰写，另外还有一卷关于组合、图论和博弈的书，由本书作者撰写.

为了节省读者翻阅的时间，参考文献（有时是范围广泛的文献资料）放在每一个问题的末尾，或放在一组问题的综述中.

有许多人看过本书的部分手稿，与作者通过信并给出过有益的评论，其中有一些是已去世的友人；Harold Davenport，Hans Heibronn，Louis Mordell，Leo Moser，Theodor Motzkin，Alfred Rényi 和 Paul Turán. 此外还有 H. L. Abbott，J. W. S. Cassels，J. H. Conway，P. Erdös，Martin Gardner，R. L. Graham，H. Halberstam，D. H. Lehmer，Emma Lehmer，A. M. Odlyzko，Carl Pomerance，A. Schinzel，J. L. Selfridge，N. J. A. Sloane，E. G. Straus，H. P. F. Swinnerton-Dyer 和 Hugh Williams. 由加拿大国立（科学和工程）研究理事会提供的资助，使我们有条件与上述各位及其他许多人取得联系. 在本书最后定稿的过程中，

卡尔加里（Calgary）大学授予的 Killam Resident 研究基金给了我特别有用的帮助. 书稿的打印工作是由 Karen Mcdermid，Betty Teare 和 Louise Guy 完成的，他们还帮忙做了校对. 此外，纽约的斯普林格出版分社的全体职员诚挚有礼、称职能干，对我们助益良多.

尽管有这些帮助，书中难免会有许多错误，对此我承担全部责任. 无论如何，只要本书服务其目的，那么它从问世的那一刻起就已经过时了，而且一旦写作开始，它就已经在变得过时. 有鉴于此，我乐于听到来自读者的声音，因为一定会有许多我所不知道的解、文献以及问题. 我希望各位能借交流有关的信息而获益. 有一些出色的研究工作者通过自己重新发现这些结果而在事业上兴旺发达起来，但我们中的许多人在了解到自己的发现已早为他人所为后变得沮丧而失望.

R. K. 盖伊

1981. 8. 13 于卡尔加里

目　录

符　　号

A.P.	算术级数 $a, a+d, \cdots, a+kd, \cdots$	A6,E10,E33
$a_1 \equiv a_2 \pmod b$	a_1 同余于 a_2(modulo d),即 a_1-a_2 被 b 整除	A3,A4,A12,A15,B2,B4,B7,…
$A(x)$	一个数列中不超过 x 的元素个数,例如不超过 x 的亲和数的个数	B4,E1,E2,E4
c	正常数	A1, A3, A8, A12, B4,B11,…
d_n	相邻素数差 $p_{n+1}-p_n$	A8,A10,A11
$d(n)$	n 的(正)因子个数,即 $\sigma_0(n)$	B, B2, B8, B12, B18, …
$d \mid n$	d 整除 n,n 是 d 的倍数,存在一个整数 q 使 $dq=n$	B, B17, B32, B37, B44,C20,D2,E16
$d \nmid n$	d 不整除 n	B, B2, B25, E14, E16,…
e	自然对数的底,2.718281828459045…	A8,B22,B39, D12,…
E_n	Euler 数,sec x 的级数展开式中的系数	B45
exp{ }	指数函数	A12, A19, B4, B36,B39,…

F_n	Fermat 数，$2^{2^n}+1$	A3，A12
$f(x)\sim g(x)$	$\frac{f(x)}{g(x)}\to 1(x\to\infty)(f,g>0)$	A1，A3，A8，B33，B41，C1，C17，D7，E2，E30，F26
$f(x)=o(g(x))$	$\frac{f(x)}{g(x)}\to 0(x\to\infty)(g>0)$	A1，A18，A19，B4，C6，C9，C11，C16，C20，D4，D11，E2，E14，F1
$f(x)=O(g(x))$	（即 $f(x)\ll g(x)$）存在一个 c 使对所有充分大的 x 有 $\lvert f(x)\rvert<cg(x)(g(x)>0)$	A19，B37，C8，C9，C10，C12，C16，D4，D12，E4，E8，E20，E30，F1，F2，F16
		A4，B4，B18，B32，B40，C9，C14，D11，E28，F4
$f(x)=\Omega(g(x))$	存在一个 $c>0$ 使得有任意大的 x 存在使 $\lvert f(x)\rvert\geqslant cg(x)(g(x)>0)$	D12，E25
$f(x)\asymp g(x)$	（即 $f(x)=\Theta(g(x))$）存在 c_1，c_2 使对所有充分大的 x 有 $c_1 g(x)\leqslant f(x)\leqslant c_2 g(x)(g(x)>0)$	B18 E20
i	-1 的平方根，$i^2=-1$	A16
$\ln x$	x 的自然对数	A1，A2，A3，A5，A8，A12，…

(m,n)	m 和 n 的最大公约数 g.c.d.， m 和 n 的最高公因子 h.c.f.	B3,B4,B5,B11,D2
$[m,n]$	m 和 n 的最大公约数 l.c.m.， 也用来代表相连整数 $m,m+1,\cdots,n$ 的集合	B35,E2,F14 B24,B26,B32,C12,C16
$m\perp n$	m 和 n 互素 $(m,n)=1$	A,A4,B3,B4,B5,B11,D2
M_n	Mersenne 素数 2^n-1	A3,B11,B38
$n!$	n 的阶乘；$1\times2\times3\times\cdots\times n$	A2,B12,B14,B22,B23,B43,…
$!n$	$0!+1!+2!+\cdots+(n-1)!$	B44
$\left[\begin{matrix}n\\k\end{matrix}\right]$	从 n 个元素中任取 k 个元素的取法数，二项系数 $\frac{n!}{k!(n-k)!}$	B31,B33,C10,D3
$\left(\frac{p}{q}\right)$	Legendre(或 Jacobi)符号	见 F5(A1,A12,F7)
$p^a \parallel n$	p^a 整除 n，但 p^{a+1} 不整除 n	B,B8,B37,F16
p_n	第 n 个素数，其中 $p_1=2$，$p_2=3$，$p_3=5$，…	A2,A5,A14,A17,E30
$p(n)$	n 的最大素因子	B30,B46
Q	有理数域	D2,F7
$r_k(n)$	不超过的数中必定包含一个有个项的算术级数的数的最少个数	见 E10
$s(n)$	n 的除去 n 以外的所有正因	B,B1,B2,B8,B10,…

	子之和，$\sigma(n)-n$	
$s^k(n)$	$s(n)$的第 k 次迭代	B，B6，B7
$s^*(n)$	如果 $d\mid n$ 且$\left(d,\frac{n}{d}\right)=1$，则称 d 为 n 的一个单因子. $s^*(n)$表示 n 的除去 n 以外的所有单因子的和	B8
$S\cup T$	集合 S 与 T 的并	E7
$W(k,l)$	van der Waerden 数	见 E10
$\lfloor x\rfloor$	x 的底，即不大于 x 的最大整数	A1，A5，C7，C12，C15，…
$\lceil x\rceil$	x 的顶，即不小于 x 的最小整数	B24
Z	整数…，−2，−1，0，1，2，…	F14
Z_n	整数环 0，1，2，…，$n-1$ $(\mathrm{mod}\,n)$	E8
γ	Euler 常数，0.577215664901532…	A8
ε	任意小的正常数	A8，A18，A19，B4，B11，…
ζ_p	p 次单位根	D2
$\zeta(s)$	Riemann ζ 函数；$\sum_{n=1}^{\infty}\frac{1}{n^s}$	D2
π	圆的周长与直径之比；3.141592653589793…	F1，F17
$\pi(x)$	不超过 x 的素数个数	A17，E4
$\pi(x;a,b)$	不超过 x 且模 b 与 a 同余的素数个数	A4
$\prod$	乘积	A1，A2，A3，A8，A15，…

$\sigma(n)$	n 的所有因子之和；即 $\sigma_1(n)$	B，B2，B5，B8，B9，…
$\sigma_k(n)$	n 的所有因子的 k 次幂之和	B，B12，B13，B14
$\sigma^k(n)$	$\sigma(n)$的第 k 次迭代	B9
$\sigma^*(n)$	n 的所有单因子之和	B8
$\sum$	求和	A5，A8，A12，B2，B14，…
$\varphi(n)$	Euler φ 函数；不超过 n 且与 n 互素的正整数的个数	B8，B11，B36，B38，B39，…
$\varphi^k(n)$	$\varphi(n)$的第 n 次迭代	B41
ω	1 的三次复根，即 $\omega^3=1$，$\omega\neq1$，$\omega^2+\omega+1=0$	A16
$\omega(n)$	n 的不同素因子的个数	B2，B8，B37
$\Omega(n)$	n 的所有素因子的个数（按重数计算）	B8
¿ ... ?	猜想或假设的命题	A1，A9，B37，C6，E10，E28，F2，F18

引　言

长期以来，无论对数学业余爱好者还是职业数学工作者来说，数论比其他任何数学分支都更有吸引力．以致现在它的许多部分都有相当的技术性困难．然而，仍有比以前更多的未解决的问题，其中许多问题虽然不太可能在下一代手中得到解决，这仍无法阻止人们去尝试．未解决的问题是如此之多，连整整一卷书也装不下它们．现在的这本书只不过是作者本人选出的一些范例．

数论中问题的一些可靠的出处曾列在本书第一版的引言中，其中的一部分重新列在下面，同时还列出了一些较新的资料．

Paul Erdös, Problems and results in combinatorial number theory III, *Springer Lecture Notes in Math.*, **626**(1977) 43～72; *MR* **57** ＃12442.

Paul Erdös, A survey of problems in combinatorial number theory, in *Combinatorial Mathematics, Optimal Designs and their Applications* (Proc. Symp. Colo. State Univ. 1978) *Ann. Discrete Math.*, **6**(1980) 89—115.

Paul Erdös & R.L.Graham, *Old and New Problems and Results in Combinatorial Number Theory*, Monographies de l'Enseignement Math.No.28, Geneva, 1980.

Paul Erdös, & András Sárközy, Some solved and unsolved problems in combinatorial number theory, *Math. Slovaca*, **28** (1978) 407～421; *MR* **80I**:10001.

Paul Erdös, Problems and results in number theory, in Halberstam & Hooley (eds) Recent Progress in Analytic Number Theory, Vol. 1, Academic Press, 1981, 1～13.

H. Fast & S. Swierczkowski, *The New Scottish Book*, Wroclaw,

1946～1958.

Heini Halberstam, Some unsolved problems in higher arithmetic, in Ronald Duncan & Miranda Weston-Smith (eds.) *The Encyclopedia of Ignorance*, Pergamon, Oxford & New York, 1977, 191～203.

Victor Klee & Stan Wagon, *Old and New Unsolved Problems in Plane Geometry and Number Theory*, Math. Assoc. Of Amer. Dolciani Math. Expositions, **11**(1991).

Proceedings of Number Theory Conference, Univ. of Colorado, Boulder, 1963.

Report of Institute in the Theory of Numbers, Univ. of Colorado, Boulder, 1959.

Joe Roberts, *Lure of the Integers*, Math.Assoc. of America, Spectrum Series, 1992.

Daniel Shanks, *Solved and Unsolved Problems in Number Theory*, Chelsea, New York, 2nd ed. 1978; *MR* **80e**:10003.

W. Sierpiński, *A selection of Problems in the Theory of Numbers*, Pergamon, 1964.

Robert D. Silverman, A perspective on computational number theory, in Computers and Mathematics, *Notices Amer. Math. Soc.*, 38(1991) 562～568.

S. Ulam, *A Collection of Mathematical Problems*, Interscience, New York, 1960.

在本书中,"数"表示自然数,即

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

而 c 表示绝对正常数,每次出现时不一定都取同样的值. 我们利用 K. E. Iverson 的现已为大家熟悉的符号"底"($\lfloor\ \rfloor$)和"顶"($\lceil\ \rceil$)来分别表示"不大于……的最大整数"和"不小于……的最小整数". 一个不大熟悉的符号是用"$m \perp n$"表示"m 与 n 互素",即"$\gcd(m,n)=1$".

本书根据我个人的想法划分成 6 个部分：

A. 素数

B. 整除性

C. 堆垒数论

D. 不定方程

E. 整数序列

F. 不在上述各章中的其他问题.

A. 素　　数

可以把正整数分成三类：

单位(unit)　1

素数(prime) 2,3,5,7,11,13,17,19,23,29,31,37,…

合数(composite) 4,6,8,9,10,12,14,15,16,….

一个大于 1 的数是素数,如果它仅有的正因子是 1 和它自己；反之则称它为合数. 至少从 Euclid 开始,数学家们就对素数感兴趣了. Euclid 曾经证明了素数有无穷多个.

用 p_n 表示第 n 个素数,例如 $p_1=2$, $p_2=3$, $p_{99}=523$;用 $\pi(x)$表示不大于 x 的素数个数,例如 $\pi(2)=1$, $\pi\left(3\frac{1}{2}\right)=2$, $\pi(1000)=168$, $\pi(4\times10^{16})=1075292778753150$. 用$(m,n)$表示 m 和 n 的最大公因子(gcd),例如$(36,66)=6$,$(14,15)=1$,$(1001,1078)=77$. 如果$(m,n)=1$,就说 m 和 n 互素(coprime),记为 $m\perp n$,例如 $182\perp165$.

Dirichlet 定理告诉我们:只要 $a\perp b$,在任何算术级数(arithmetic progression)

$$a, a+b, a+2b, a+3b, \cdots$$

中必有无穷多个素数. 下文对有关素数的问题和进一步的参考资料给出了综述：

A. Schinzel & W. Sierpiński, Sur certains hypothèses concernant les nombres premiers, *Acta Arith.*, 4(1958) 185－208; erratum5(1959) 259; *MR* 21＃4936;又见 7(1961)1－8.

问题 D27 中的表 7 可以用作为小于 1000 的素数表;表中写有数字 1,3,5,7 对应的数都是素数,而 1,3,5,7 指的是该素数模 8 所在的剩余类(见 A4).

多年来，确定一个大数是素数还是合数，而在它为合数时确定它的因子这样一个一般性的问题一直吸引着数论学者．随着高速计算机的出现，问题取得了相当大的进展．近来还由于它对密码分析学的应用，对这一问题的研究又提供了新的动力．其他一些文献放在问题 A3 之后及本书第一版中．

参 考 文 献

William Adams & Daniel Shanks, Strong primality tests that are not sufficient, *Math. Comput.*, **39**(1982) 255–300.

Richard K. Guy, How to factor a number, *Congressus Numerantium XVI*, Proc. 5th Manitoba Conf. Numer. Math., Winnipeg, 1975, 49–89; *MR* **53** #7924.

Wilfrid Keller, Woher kommen die größten derzeit bekannten Primzahlen? *Mitt. Math. Ges. Hamburg*, **12**(1991) 211–229; *MR* **92j**:11006.

Arjen K. Lenstra & Mark S. Manasse, Factoring by electronic mail, in Advances in Cryptology—EUROCRYPT'89, *Springer Lect. Notes in Comput. Sci.*, **434**(1990) 355–371; *MR* **91i**:11182.

Hendrik W. Lenstra, Factoring integers with elliptic curves, *Ann. of Math.*(2), **126**(1987) 649–673; *MR* **89g**:11125.

Hendrik W. Lenstra & Carl Pomerance, A rigorous time bound for factoring integers, *J. Amer. Math. Soc.*, **5**(1992) 483–916; *MR* **92m**:11145.

G. L. Miller, Riemann's hypothesis and tests for primality, *J. Comput. System Sci.*, **13**(1976) 300–317; *MR* **58** #470ab.

Peter Lawrence Montgomery, An FFT extension of the elliptic curve method of factorization, PhD dissertation, UCLA, 1992.

J. M. Pollard, Theorems on factoring and primality testing, *Proc. Cambridge Philos. Soc.*, **76**(1974) 521–528; *MR* **50** #6992.

J. M. Pollard, A Monte Carlo method for factorization, *BIT*, **15**(1975) 331–334; *MR* **52** #13611.

Carl Pomerance, Recent developments in primality testing, *Math. Intelligencer*, **3**(1980/81) 97–105.

Carl Pomerance, Notes on Primality Testing and Factoring, *MAA Notes* **4**(1984) Math. Assoc. of America, Washington DC.

Carl Pomerance (editor), Cryptology and Computational Number Theory, *Proc. Symp. Appl. Math.*, **42** Amer. Math. Soc., Providence, 1990; *MR* **91k**: 11113.

Paulo Ribenboim, *The Book of Prime Number Records*, Springer-Verlag, New York, 1988.

Paulo Ribenboim, *The Little Book of Big Primes*, Springer-Verlag, New York, 1991.

Hans Riesel, Wie schnell kann man Zahlen in Faktoren zerlegen? *Mitt. Math. Ges. Hamburg*, **12**(1991) 253–260.

R. Rivest, A. Shamir & L. Adleman, A method for obtaining digital signatures and public key cryptosystems, *Communications A.C.M.*, Feb. 1978.
R. Solovay & V. Strassen, A fast Monte-Carlo test for primality, *SIAM J. Comput.*, **6**(1977) 84–85; erratum **7**(1978) 118; *MR* **57** #5885.
Jonathan Sorenson, Counting the integers cyclotomic methods can factor, *Comput. Sci. Tech. Report*, **919**, Univ. of Wisconsin, Madison, March 1990.
H. C. Williams & J. S. Judd, Some algorithms for prime testing using generalized Lehmer functions, *Math. Comput.*, **30**(1976) 867–886.

A1. 取素数值的二次函数

有无穷多个形如 a^2+1 的素数吗？可能如此. 事实上 Hardy 和 Littlewood(在他们的猜想 E 中)曾猜想：小于 n 的这种素数的个数 $P(n)$渐近地等于 $c\sqrt{n}/\ln n$，

$$¿\quad P(n)\sim c\sqrt{n}/\ln n\quad ?$$

即 $P(n)$与 $\sqrt{n}/\ln n$ 的比值当 $n\to\infty$时趋向于 c. 常数 c 等于

$$c=\prod\left\{1-\frac{\left(\frac{-1}{p}\right)}{p-1}\right\}=\prod\left\{1-\frac{(-1)^{(p-1)/2}}{p-1}\right\}\approx 1.3727,$$

其中$\left(\frac{-1}{p}\right)$是 Legendre 符号(见 F5)，该乘积取过所有奇素数. 对于用更为一般的二次多项式表示的素数之个数这一问题，他们做出了类似的猜想，仅仅常数 c 的值有所不同. 但是我们尚不知道有哪一个高于一次的多项式已被证明能取到无穷多个素数值. 是否对每个 $b>0$，都有一个形如 a^2+b 的素数呢？Sierpiński 曾经证明了：对每个 k，存在一个 b，使得有多于 k 个形如 a^2+b 的素数.

Iwaniec 证明了存在无穷多个 n，使 n^2+1 是至多两个素数之积. 他的结果可以推广到其他二次不可约多项式上去.

如果 $P(n)$表示 n 的最大素因子，Maurice Mignotte 证明了当 $a\geqslant 240$ 时有 $P(a^2+1)\geqslant 17$. 注意到有 $239^2+1=2\times 13^4$(这是数 239 的又一个性质). 50 年来人们就已经知道 $P(a^2+1)\to\infty$($a\to\infty$).

Ulam 和其他人注意到，当数列写成“方形螺线”时，似乎在与

某种“富含素数”的二次多项式对应的对角线上更容易出现素数. 例如,图 1 的主对角线就对应 Euler 著名的公式 n^2+n+41.

421	420	**419**	418	417	416	415	414	413	412	411	410	**409**	408	407	406	405	404	403	402
422	**347**	346	345	344	343	342	341	340	339	338	**337**	336	335	334	333	332	**331**	330	**401**
423	348	**281**	280	279	278	**277**	276	275	274	273	272	**271**	270	**269**	268	267	266	329	400
424	**349**	282	**223**	222	221	220	219	218	217	216	215	214	213	212	**211**	210	265	328	399
425	350	**283**	224	**173**	172	171	170	169	168	**167**	166	165	164	**163**	162	209	264	327	398
426	351	284	225	174	**131**	130	129	128	**127**	126	125	124	123	122	161	208	**263**	326	**397**
427	352	285	226	175	132	**97**	96	95	94	93	92	91	90	121	160	207	262	325	396
428	**353**	286	**227**	176	133	98	**71**	70	69	68	**67**	66	**89**	120	159	206	261	324	395
429	354	287	228	177	134	99	72	**53**	52	51	50	65	88	119	158	205	260	323	394
430	355	288	**229**	178	135	100	**73**	54	**43**	42	49	64	87	118	**157**	204	259	322	393
431	356	289	230	**179**	136	**101**	74	55	44	**41**	48	63	86	117	156	203	258	321	392
432	357	290	231	180	**137**	102	75	56	45	46	**47**	62	85	116	155	202	**257**	320	391
433	358	291	232	**181**	138	**103**	76	57	58	**59**	60	**61**	84	115	154	201	256	319	390
434	**359**	292	**233**	182	**139**	104	77	78	**79**	80	81	82	**83**	114	153	200	255	318	**389**
435	360	**293**	234	183	140	105	106	**107**	108	**109**	110	111	112	**113**	152	**199**	254	**317**	388
436	361	294	235	184	141	142	143	144	145	146	147	148	**149**	150	**151**	198	253	616	387
437	362	295	236	185	186	187	188	189	190	**191**	192	**193**	194	195	196	**197**	252	315	386
438	363	296	237	238	**239**	240	**241**	242	243	244	245	246	247	248	249	250	**251**	314	385
439	364	297	298	299	300	301	302	303	304	305	306	**307**	308	309	310	**311**	312	**313**	384
440	365	366	**367**	368	369	370	371	372	**373**	374	375	376	377	378	**379**	380	381	382	**383**

图 1　素数(用黑体表示者)构成对角图案

有一些次数大于 1 的(多项式)表示素数的结果,它们起源于 Pyateckii-Šapiro. 他证明了:如果 $1\leqslant c\leqslant\frac{12}{11}$,那么在范围 $1<n<x$ 中形如$\lfloor n^c\rfloor$的素数个数等于

$$(1+o(1))\,x/(1+c)\ln x.$$

其中的数$\frac{12}{11}$先后被 Kolesnik, Graham 和 Leitmann, Heath-Brown, Kolesnik 以及刘弘泉(Liu Hong-Quan)和 Rivat 相继改进为$\frac{10}{9}$, $\frac{69}{62}$, $\frac{755}{662}$, $\frac{39}{34}$和$\frac{15}{13}$.

参 考 文 献

Gilbert W. Fung & Hugh Cowie Williams, Quadratic polynomials which have a high density of prime values, *Math. Comput.*, **55**(1990) 345–353; *MR* **90j**:11090.

Martin Gardner, The remarkable lore of prime numbers, *Scientific Amer.*, **210**

#3 (Mar. 1964) 120–128.

G. H. Hardy & J. E. Littlewood, Some problems of 'partitio numerorum' III: on the expression of a number as a sum of primes, *Acta Math.*, **44**(1922) 1–70.

D. R. Heath-Brown, The Pyateckii-Šapiro prime number theorem, *J. Number Theory*, **16**(1983) 242–266.

D. R. Heath-Brown, Zero-free regions for Dirichlet L-functions, and the least prime in an arithmetic progression, Proc. London Math. Soc.(3) **64**(1992) 265–338.

Henryk Iwaniec, Almost-primes represented by quadratic polynomials, *Invent. Math.*, **47**(1978) 171–188; *MR* **58** #5553.

G. A. Kolesnik, The distribution of primes in sequences of the form $[n^c]$, *Mat. Zametki*(2), **2**(1972) 117–128.

G. A. Kolesnik, Primes of the form $[n^c]$, *Pacific J. Math.*(2), **118**(1985) 437–447.

D. Leitmann, Abschätzung trigonometrischer Summen, *J. reine angew. Math.*, **317**(1980) 209–219.

D. Leitmann, Durchschnitte von Pjateckij-Shapiro-Folgen, *Monatsh. Math.*, **94**(1982) 33–44.

H. Q. Liu & J. Rivat, On the Pyateckii-Šapiro prime number theorem, *Bull. London Math. Soc.*, **24**(1992) 143–147.

Maurice Mignotte, $P(x^2+1) \geq 17$ si $x \geq 240$, *C. R. Acad. Sci. Paris Sér. I Math.*, **301**(1985) 661–664; *MR* **87a**:11026.

Carl Pomerance, A note on the least prime in an arithmetic progression, *J. Number Theory*, **12**(1980) 218–223.

I. I. Pyateckii-Šapiro, On the distribution of primes in sequences of the form $[f(n)]$ (Russian), *Mat. Sbornik N.S.*, **33**(1953) 559–566; *MR* **15**, 507.

Daniel Shanks, On the conjecture of Hardy and Littlewood concerning the number of primes of the form n^2+a, *Math. Comput.*, **14**(1960) 321–332.

W. Sierpiński, Les binômes x^2+n et les nombres premiers, *Bull. Soc. Roy. Sci. Liège*, **33**(1964) 259–260.

E. R. Sirota, Distribution of primes of the form $p=[n^c]=[t^d]$ in arithmetic progressions (Russian), *Zap. Nauchn. Semin. Leningrad Otdel. Mat. Inst. Steklova*, **121**(1983) 94–102; *Zbl.* **524**.10038.

A2. 与阶乘有关的素数

是否有无穷多个形如 $n!\pm 1$ 的素数？或无穷多个形如

$$X_k = 1 + \prod_{i=1}^{k} p_i$$

的素数？或无穷多个形如 $X_k - 2$ 的素数？Buhler, Crandall 和 Penk 证明了：当 $n=1,2,3,11,27,37,41,73,77,116,154,320,340,399,427$ 时 $n!+1$ 是素数；对 $n<546$，仅当 $n=3,4,6,7,12,$

14,30,32,33,38,94,166,324,379,469 时 $n!-1$ 才是素数;对 $p_k<3088$,仅当 $p_k=2,3,5,7,11,31,379,1019,1021,2657$ 时 X_k 才是素数;当 $p_k=3,5,11,13,41,89,317,337,991,1873,2053$ 时 X_k-2 是素数;而当 $p_k=2377$ 时 X_k-2 有可能是素数(尚未对此作出检验). Harvey Dubner 发现 $872!+1$ 和 $1477!+1$ 是素数,而对 $p_k=3229,4547,4787$, X_k 是素数. 又对 $p_k=11549$ 和 13649, X_k 仍为素数.

令 q_k 表示大于 X_k 的最小素数. R. F. Fortune 曾猜想,对所有 k, q_k-X_k+1,都是素数(这样的素数称为吉祥素数,见下文——译者注). 显然,它不能被前 k 个素数整除. Selfridge 注意到:这一猜想的正确性可以从 Schinzel 关于 Cramér 猜想的一种表述推导出来. Cramér 猜想是说,对 $x>8$,在 x 和 $x+(\ln x)^2$ 之间总有一个素数. 基于如下的假设:所涉及的很大的可能是素数的数皆为真正的素数,Stan Wagon 计算出了前 100 个吉祥素数:

3 5 7 13 23 17 19 23 37 61 67 61 71 47 107 59 61 109 89 103
79 151 197 101 103 233 223 127 223 191 163 229 643 239 157 167 439 239 199 191
199 383 233 751 313 773 607 313 383 293 443 331 283 277 271 401 307 331 379 491
331 311 397 331 353 419 421 883 547 1381 457 457 373 421 409 1061 523 499 619 727
457 509 439 911 461 823 613 617 1021 523 941 653 601 877 607 631 733 757 877 641

这一问题的答案也许是肯定的,但是在可以看得见的未来,无论是用计算机还是解析工具,都不大可能解决这些猜想. Schinzel 猜想归因于 Cramér,而 Cramér 猜测有(见 A8 的参考文献)

$$¿\quad \limsup_{n\to\infty}\frac{p_{n+1}-p_n}{(\ln p_n)^2}=1\quad ?$$

Schinzel 注意到:即使对充分大的 x,这个结果也并不能蕴含 x 与 $x+(\ln x)^2$ 之间必有素数存在. 更有希望成立但仍难以证明的是下述的 Erdös 和 Stewart 的猜想:使得

$$n!+1=p_k^a p_{k+1}^b,\quad p_{k-1}\leqslant n<p_k$$

成立的仅有的情形是 $1!+1=2$, $2!+1=3$, $3!+1=7$, $4!+1$

$=5^2$,5！$+1=11^2$ 吗(注意在这五种情形有$(a,b)=(1,0),(1,0),(0,1),(2,0)$和$(0,2)$)?

Erdös 又问道:是否存在无穷多个素数 p,使对满足 $1\leqslant k!<p$ 的每个 k,$p-k!$ 皆为合数? 例如 $p=101$ 和 $p=211$. 他认为也许求解下列问题会更容易一些:存在无穷多个整数 $n(l!<n\leqslant(l+1)!)$,它们的素因子均大于 l,且所有的数 $n-k!$ $(1\leqslant k\leqslant l)$皆为合数.

参 考 文 献

I. O. Angell & H. J. Godwin, Some factorizations of $10^n\pm1$, *Math. Comput.*, **28**(1974) 307–308.

Alan Borning, Some results for $k!\pm1$ and $2\cdot3\cdot5\cdots p\pm1$, *Math. Comput.*, **26**(1972) 567–570.

J. P. Buhler, R. E. Crandall & M. A. Penk, Primes of the form $n!\pm1$ and $2\cdot3\cdot5\cdots p\pm1$, *Math. Comput.*, **38**(1982) 639–643; corrigendum, Wilfrid Keller, **40**(1983) 727; *MR* **83c**:10006, **85b**:11119.

Harvey Dubner, Factorial and primorial primes, *J. Recreational Math.*, **19** (1987) 197–203.

Martin Gardner, Mathematical Games, *Sci. Amer.*, **243**#6(Dec. 1980) 18–28.

Solomon W. Golomb, The evidence for Fortune's conjecture, *Math. Mag.*, **54**(1981) 209–210.

S. Kravitz & D. E. Penney, An extension of Trigg's table, *Math. Mag.*, **48**(1975) 92–96.

Mark Templer, On the primality of $k!+1$ and $2*3*5*\cdots*p+1$, *Math. Comput.*, **34**(1980) 303–304.

A3. Mersenne 素数,循环整数,Fermat 数,形如 $k\cdot2^n+2$ 的素数

特殊形状的素数有永恒的兴趣,特别是 **Mersenne 素数** (Mersenne prime)2^p-1. 这里 p 必须是素数,但这并不是使 2^p-1 为素数的充分条件! 例如 $2^{11}-1=2047=23\cdot89$. 它们与完全数有关(见 B1).

强有力的 Lucas-Lehmer 判别法以及不断升级换代的计算机和使用计算机的更加成熟的技术,使形如 2^p-1 的素数表不断扩大: