数论中的问题与结果

曹珍富　编著

哈尔滨工业大学出版社

内容简介

本书几乎囊括了数论中的全部历史与现代问题，同时对这些问题研究的结果与发表论文的出处作了详细介绍。

全书共六章，分别为：素数、整除、堆垒数论、丢番图方程、整数序列以及一些其它问题。本书是在编译理查德 K. 盖依(Richard K. Guy)所著《数论中尚未解决的问题》(Unsolved Problems in Number Theory)的基础上增加新的问题与结果，同时作适当删减而写成的。其中完全新写的内容有 A18、D2、D5、D9、D25、D26、D27、D28、E28、F20、F30 等。

本书可作为数学工作者、研究生、大学生以及数学爱好者阅读与参考。

数论中的问题与结果

Shulunzhong de Wenti yu Jiegou

曹珍富　编著

*

哈尔滨工业大学出版社出版

新华书店首都发行所发行

哈尔滨市工大节能印刷厂印刷

*

开本 850×1168　1/32　印张 8　　字数 230 千字

1996 年 6 月第 1 版　　1998 年 4 月第 2 次印刷

印数　1 501—2 500

ISBN 7-5603-1152-0/O・76　定价 12.00 元

前　言

数论是一门古老的数学分支。由于它的问题简明易懂，因此它比任何一个其它数学分支都更吸引人们的注意。许多业余数学爱好者都是从这里起步，通过对数论中的一些问题的探讨，获得了从事数学研究的信心。这一点对初做研究的人来说是非常重要的。

在许多数论问题的研究中我国都处于领先地位，而且自古以来，我们的祖先就已从事数论中某些问题的研究，取得了举世瞩目的成果。象闻名于世的孙子定理（又称中国剩余定理），它不仅是初等数论中的一个精美定理，而且在计算机科学、通信理论等现代科学技术领域中也得到了相当广泛的应用。早在商高年代，我们的祖先就知道"勾三股四而弦五"的结论，即给出了方程 $x^2+y^2=z^2$ 的一组正整数解 $x=3, y=4, z=5$。这要比古希腊三世纪的丢番图(Diophantus)研究这类方程早多了。在我国现代的数学家中，华罗庚、柯召、闵嗣鹤等老一辈数论学家曾取得过辉煌成就。其中尤以华罗庚教授在解析数论上的工作，是举世公认的。60 年代以来，我国数论学家陈景润、王元、潘承洞等，在筛法与哥德巴赫(Goldbach)猜想等问题上取得了国际上领先的结果。受到他们的鼓舞，我国年轻的数论工作者在许多问题上也取得一系列的新进展。为了使更多的人了解数论中的问题与结果，我在 1987 年 10 月编译了理查德 K. 盖依(Richard K. Guy)著《数论中尚未解决的问题》(Unsolved Problems in Number Theory, Springer-Verlag, New York, 1981)，但由于种种原因没有出版。鉴于盖依教授的书写得非常好，我认为值得向国内广大数学工作者与数学爱好者推荐。现

在，许多问题有了新的进展，而且又有许多新问题被提出来，所以丰富与发展盖依教授的书就是件很有意义的事。本书就是在当时编译书稿的基础上改写的，在保留了原书参考文献的基础上，又增加了许多新文献，并且在原书的框架下，几乎对每个问题均进行了重写，删掉了个别含模不清的问题，同时增加了若干新的问题与结果，其中有些章节是完全新增的，比如 A18，D2，D5，D9，D25，D26，D27，D28，E28，F20，F30 等等。

全书共分六章，分别为素数、整除、堆垒数论、丢番图方程、整数序列以及一些其它问题。

应该指出，由于本书成稿大部分在七年前，虽然这次改写尽了全力，但仍会有挂一漏万之处，特别是在本书即将出版之际，国内外许多新的问题与结果正在不断涌现，现已没有精力增写这部分内容，也不可能跟上这样一种步伐。

我由衷地感谢对本书的出版给予支持、帮助的各界朋友。黑龙江省省长田凤山在任哈尔滨市市长时就给予明确指示，尽快出版此书。哈尔滨市科委、轻工局对本书的出版均给予了支持与帮助。当时在哈尔滨工业大学读研究生的江卫民和唐虎林二位同志，在本书原稿的编译过程中自始至终给予了极大的帮助，尤其是江卫民同志，在翻译初稿和抄稿上协助做了大量的工作，借此机会一并向他们致以诚挚的感谢！

曹珍富

于哈尔滨 1994.5.20

目　录

A 素数

我们把正整数分成三类：

单位数：1

素数：2,3,5,7,11,13,17,19,23,29,31,37,…

合数：4,6,8,9,10,…

如果一个大于1的数仅有的正约数是1和它本身，便称这个数为素数；否则称为合数. Euclid 证明了素数个数无限，因此，至少从 Euclid 起，素数就已经引起了数学家的兴趣.

通常用 p_n 表示第 n 个素数，如 $p_1=2,p_2=3,p_{99}=523$，用 $\pi(x)$ 表不超过 x 的素数个数，例如 $\pi(2)=1,\pi(3.5)=2,\pi(1000)=168$. m,n 的最大公约数($g.c.d$)用 (m,n) 表示，如果 $(m,n)=1$，则称 m,n 互素.

Dirichlet 证明了，当 $(a,b)=1$ 时，算术级数

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

中有无限多个素数. Schinzel 和 Sierpinski 曾写过一篇综述素数问题的文章，其中给出了大量的参考文献.

在本书问题 D23 的表 7 中给出了小于 1000 的素数表.

许多世纪以来，一直吸引着许多数论家注意的问题是：怎样确定一个大数是素数还是合数？如果是合数，那么它的因子又是什么？随着高速计算机的出现，这一问题已取得了可观的进展，而密码分析的需要又更进一步促进了它的发展.

本书中我们总用 c 表示正常数，用 $\langle x\rangle$ 表示不小于 x 的最小整数，而用 $[x]$ 表示不大于 x 的最大整数.

[1]Leonard Adleman and Frank Thomson Leighton, An $O(n^{1/10.89})$ primality

testing algorithm, *Math. Comp.*, 36(1981), 261-266.

[2]R. P. Brent, An improved Monte Carlo factorization algorithm, *BIT*, 20 (1980), 176-184.

[3]曹珍富(Z. Cao), 公钥密码学, 黑龙江教育出版社, 1993.

[4]John D. Dixon, Asymptotically fast factorization of integers, *Math. Comp.*, 36(1981), 255-260.

[5]Richard K. Guy, How to factor a number, *Congressus Numerantiun XVI* Proc. 5th Manitoba Conf. Numer. Math., Winnipeg, 1975, 49-89.

[6]H. W. Lenstra, Primality testing. *Studieweek Getaltheorie en Computers*, Stichting Mathematisch Centrum, Amsterdam, 1980, 41-60.

[7]G. L. Miller, Riemann's hypothesis and tests for primality, *J. Comput. System Sci*, 13(1976), 300-317.

[8]J. M. Pollard, Theorems on factorization and primality testing, *Proc. Cambridge Philos. Soc*, 76(1974), 521-528.

[9]J. M. Pollard, A Monte Carlo method for factorization, *BIT*, 15(1975), 331-334, *MR* 50#6992.

[10]R. Rivest, A. Shamir and L. Adleman, A method for obtaining digital signatures and public key cryptosystems, *Communications A. C. M*, Feb. 1978.

[11]A. Schinzel and W. Sierpinski, Sur certains hypotheses concernant les nombres premiers, *Acta Arith.*, 4 (1958) 185-208 (erratum5 (1959) 259); *MR* 21#4036.

[12]R. Solovay and V. Strassen, A fast Monte-Carlo test for primality, *SIAM J. Comput*, 6(1977), 84-85; erratum 7 (1978), 118; *MR* 57#5885.

[13]H. C. Williams, Primality testing on a computer, *Ars Combin.*, 5(1978), 127-185; *MR* 80d:10002.

[14]H. C. Williams and R. Holte, Some observations on primality testing, *Math. Comp.*, 32(1978), 905-917; *MR* 57#16184.

[15]H. C. Williams and J. S. Judd, Some algorithms for prime testing using generalized Lehmer functions, *Math Comp.*, 30(1976), 867-886.

A1. 二次函数的素数值

形如 a^2+1 的素数有无限多吗？Hardy 和 Littlewood(他们的猜想 E)猜测：比 n 小的这样的素数个数 $p(n)$ 渐近于 $c\sqrt{n}/\ln n$，即 $p(n)\sim c\sqrt{n}/\ln n$，就是说，当 $n\to\infty$ 时，$p(n)$ 与 $\sqrt{n}/\ln n$ 的比值趋于一个常数 c，这个常数是：

$$c=\prod_p\{1-\frac{(\frac{-1}{p})}{p-1}\}=\prod_p\{1-\frac{(-1)^{(p-1)/2}}{p-1}\}\approx 1.3727$$

其中，$(\frac{-1}{p})$ 是 Legendre 符号(见 F5)，且 $\prod_p$ 取遍所有奇素数. 对用更一般的二次表达式表示的素数个数，它们俩作了类似的猜想，唯一的差别只是 c 值不同. 但是，我们不知道一般的次数大于 1 的整值多项式(一次多项式已证明可取无穷多个素数)如何，甚至对每一个 $b>0$ 是否都有一个形如 a^2+b 的素数也没有解决.

Iwaniec 已证明，存在无穷多个 n，使 n^2+1 至多为两个素数的乘积. 他的结果可推到另外一些不可分解的二次多项式上.

Ulam 和其他人注意到，当整数序列按方螺旋形式(参见图 1)

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 85 116 155 201 **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** 198 253 316 387
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(黑体字)形成的对角线型

写出时，素数形成的图形似乎是一些对角线，每一对角线对应一个特定的含素数丰富的二次多项式. 例如，图 1 的主对角线与 Euler 的著名多项式 n^2-n+41 相对应. Rabinovitch 和陆洪文发现了更一般的事实，这些事实由类数 1 的虚或实的二次域决定，例如 Euler 多项式是 Rabinovitch 的特例，陆洪文的多项式为 N^2-n-n^2，这里 $N>1$ 使得二次域 $Q(\sqrt{4N^2+1})$ 的类数为 1. 例如 $N=13$ 符合要求，故当 $n=1,2,\cdots,12$ 时 $169-n-n^2$ 均是素数.

[1] Martin Gardner, The remarkable lore of prime numbers, *Scientific Amer.*, 210#3(Mar. 1964), 120-128.

[2] G. H. Hardy and 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.

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

[4] 陆洪文(H. Lu)，关于实二次域的类数，科学通报，24(1979)，4：149－150.

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

A2. 与阶乘有关的素数

形如 $n!+1$ 的素数是否有无限多个？当 $n\leqslant 230$ 时，使 $n!+1$ 为素数的 n 值仅仅是 1,2,3,11,27,37,41,73,77,116 和 154. 形如 $n!-1$ 或 $x=1+\prod_{i=1}^{k}p_i$ 的素数是否也为无限多个？当 $p_k\leqslant 1031$ 时，x 为素数的仅有的 p_k 值是 2,3,5,7,11,31,379,1019 和 1021.

设 q 是大于 x 的最小素数，R. F. Fortune 猜想，对于所有的 k，$q-x+1$ 是素数. 显然，它不能被前 k 个素数除尽. Selfridge 注意到，Fortune 猜想的真实性依赖于 Schinzel 的一个猜想，即，对 $x>8$，在 x 和 $x+(\ln x)^2$ 间总存在一个素数. 目前已知的 $q-x+1$ 形的数都是素数，它们随 $k=1,2,3,\cdots$ 分别是 3,5,7,13,23,17,19,

23,37,61,67,61,71,47,107,59,61,109,89,103,79,… 因此，很可能 Fortune 猜测的答案是“对”. 但是，短时期内在计算机或分析工具力所能及的范围内，这种的猜测的证明仍似乎是不可想象的.

有希望解决但仍然很困难的是下面的 Erdös 和 Stewart 猜想：$1!+1=2, 2!+1=3, 3!+1=7, 4!+1=5^2, 5!+1=11^2$ 是 $n!+1=p_k^a p_{k+1}^b$ 且 $p_{k-1}\leqslant n<p_k$ 的仅有的几种情形吗？[注意，在上述五种情形里，$(a,b)=(1,0),(1,0),(0,1),(2,0)$ 和 $(0,2)$]

Erdös 又问，是否存在无穷多个素数 p，对每一个 $k(1\leqslant k!<p)$ 均有 $p-k!$ 是合数？例如，对 $p=101$ 和 $p=211$，$p-k!(1\leqslant k<p)$ 都是合数. 他认为下面的一个问题也许更易于证明：是否有无穷多个整数 $n(l!<n\leqslant(l+1)!)$，其所有素因子均大于 l，且所有 $n-k!(1\leqslant k\leqslant l)$ 是合数.

David Silverman 注意到，当 $m=1,2,3,4$ 和 8 时，乘积 $\prod_{i=1}^{m}\frac{p_i+1}{p_i-1}$ 是整数，他问是否还有其它的 m 使上述乘积为整数.

[1]I. O. Angell and H. J. Godwin, Some factorizations of $10^n\pm1$, *Math. Comp.*, 28(1974), 307-308

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

[3]Martin Gardner, Mathematical Games, *Sci. Amer.*, 243 # 6(Dec. 1980), 18-28.

[4]S. Kravitz and D. E. Penney, An extension of Trigg's table, *Math. Mag.*, 48(1975), 92-96.

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

A3. Mersenne 素数与 Fermat 数

人们对具有特定形式的素数一直抱有兴趣，特别是对与完全数（见 B1）相联系的 Mersenne 素数 2^p-1（这里 p 必然是素数，但不

是充分条件!例如,$2^{11}-1=2047=23\times 89$),以及 Repunit 素数 $(10^p-1)/9$.

借助于计算机及在使用计算机时用一些更为复杂的技术,Lucas—Lehmer 试验不断地增加着,得到这样一个素数表(对素数表中的每一个 p,2^p-1 也是素数):2,3,5,7,13,17,19,31,61,89,107,127,521,607,1279,2203,2281,3217,4253,4423,9689,9941,11213,19937,21701,23209,44497,86243,132049,216091,… 无疑地,他们的个数将会是无穷多.但是,要证明它却毫无希望.假定 $M(x)$ 是素数 $p\leqslant x$ 使 2^p-1 为素数的个数.对 $M(x)$ 的大小,我们希望找到一个令人信服的直观推断.Gillies 认为 $M(x)\sim c\ln x$.但有些人不相信它.

D. H. Lehmer 置 $S_1=4$,$S_{k+1}=S_k^2-2$,假定 2^p-1 是一个 Mersenne 素数,注意到 $S_{p-2}\equiv 2^{(p+1)/2}$ 或 $-2^{(p+1)/2}(\mathrm{mod}\ 2^p-1)$,他问:$S_{p-2}\equiv 2^{(p+1)/2}(\mathrm{mod}\ 2^p-1)$ 还是 $S_{p-2}\equiv -2^{(p+1)/2}(\mathrm{mod}\ 2^p-1)$?

Selfridge 猜测,如果 n 是形如 $2^k\pm 1$ 或 $2^{2k}\pm 3$ 的素数,那么,2^n-1 和 $(2^n+1)/3$ 两者要么全是素数,要么全不是.此外,如果 2^n-1 和 $(2^n+1)/3$ 都是素数,那么 n 便具有 $2^k\pm 1$ 或 $2^k\pm 3$ 的形式之一.一个新的 Mersenne 猜想是,如果下面三条中两条是正确的,那么第三条也正确:(a)$n=2^k\pm 1$ 或 $n=4^k\pm 3$;(b)2^n-1 是素数;(c)$(2^n+1)/3$ 是素数.这个新猜想对于 $n<10^5$ 是正确的(参见[4]).Mullin 推广了这个猜想.设 P,Q 是两个互素的非零整数,$P^2-4Q\neq 0$,再设 a,b 是方程 $x^2-Px+Q=0$ 的两个根,定义 $u_n=(a^n-b^n)/(a-b)(n\geqslant 0)$,$v_n=(a^n+b^n)/(a+b)$($n$ 奇),则 Mullin 提出的更一般猜想是,如果下面三条中两条是正确的,那么第三条也是正确的:(a)$n=2^k\pm 1$ 或 $4^k\pm 3$;(b)u_n 是一个素数;(c)v_n 是一个素数.

如果 p 是素数,那么 2^p-1 总是无平方因子吗?这似乎又是一个不可回答的问题.回答"不"是安全的.如果你运气的话,这个问题

也许能由计算机解出. 正如 D. H. Lehmer 在谈到各种分解方法时所说的:"机遇恰在角落周围徘徊."Selfridge 正确地以一个问题表述上面那个问题计算上的困难性:"试找到 50 或更多个象 1093 和 3511 的素数"(这两个素数 p 是仅有的比 3×10^9 小且它们平方能除尽 2^p-2 的素数).

与 $(10^p-1)/9$ 是素数对应的 p 值已知的有 2,19,23,317,1031,最后两个是 Hugh Williams 最近发现的. 大于 1 的 Repunit 数决不可能是平方数和立方数,这可由 Ljunggren 关于丢番图方程 $\frac{x^n-1}{x-1}=y^q$ 的结果立即推出. 但是,我们不知道什么时候它们是无平方因子数.

Fermat 数 $F_n=2^{2^n}+1$ 也一直是人们感兴趣的. 对于 $0\leqslant n\leqslant 4$,F_n 均是素数,对于 $5\leqslant n\leqslant 19$ 和许多更大的 n,F_n 为合数. Hardy 和 Wright 给出了一个直观的推断:Fermat 数中仅有有限个是素数. Selfridge 更支持如下猜想:所有其他的 Fermat 数全为合数. 王元(1979)指出:F_{14} 是目前未知其任何素因子的最大复合数.

由于形如 $k2^n+1$ 的数极有可能成为 Fermat 数的因子,因此,它们也受到了特别的注意,至少对 k 较小时是如此. 例如,Hugh Williams 发现,如果 $k=5$,那么 $n=3313$,4678 和 5947 时,$k\cdot 2^n+1$ 是素数,且第一个能除尽 F_{3310}. 另外,Richard Brent 已证明,$p=1238926361552897$ 除尽 F_8(参见 B19).

我们不大可能确切知道 Fibonacci 序列:

1,1,2,3,5,8,13,21,34,55,89,144,233,377,610,987,1597,…

(其中 $u_1=u_2=1$,$u_{n+1}=u_n+u_{n-1}$)$(n\geqslant 2)$ 是否包含有无穷多个素数. 类似地,对于相关的 Lucas 序列:1,3,4,7,11,18,29,47,76,123,199,322,521,843,1364,…和其他更多的由二次递推关系式定义的 Lucas－Lehmer 序列 $((u_1,u_2)=1)$,情况是否也是如此呢? 但是,Graham 已证明,Lucas－Lehmer 序列当:

$u_1=1786\ 772701\ 928802\ 632268\ 715130\ 455793$