国外数学名著系列
（影印版）29

Richard K. Guy

Unsolved Problems in Number Theory

Third Edition

数论中未解决的问题

（第三版）

科学出版社
www.sciencep.com

国外数学名著系列(影印版) 29

Unsolved Problems in Number Theory

Third Edition

数论中未解决的问题

(第三版)

Richard K. Guy

科学出版社
北京

图字:01-2006-7383

Richard K. Guy: Unsolved Problems in Number Theory(Third Edition)

图书在版编目(CIP)数据

数论中未解决的问题:第3版=Unsolved Problems in Number Theory (Third Edition)/(加)盖伊(Guy, R. K.)著.—影印版.—北京:科学出版社,2007

(国外数学名著系列)

ISBN 978-7-03-018293-7

Ⅰ.数… Ⅱ.盖… Ⅲ.数论-研究-英文 Ⅳ.O156

中国版本图书馆CIP数据核字(2006)第153197号

责任编辑:范庆奎/责任印刷:安春生/封面设计:黄华斌

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

中国科学院印刷厂 印刷

科学出版社发行 各地新华书店经销

*

2007年1月第 一 版 开本:B5(720×1000)

2007年1月第一次印刷 印张:28 3/4

印数:1—3 500 字数:538 000

定价:78.00元

(如有印装质量问题,我社负责调换〈科印〉)

《国外数学名著系列》(影印版)序

要使我国的数学事业更好地发展起来，需要数学家淡泊名利并付出更艰苦地努力。另一方面，我们也要从客观上为数学家创造更有利的发展数学事业的外部环境，这主要是加强对数学事业的支持与投资力度，使数学家有较好的工作与生活条件，其中也包括改善与加强数学的出版工作。

从出版方面来讲，除了较好较快地出版我们自己的成果外，引进国外的先进出版物无疑也是十分重要与必不可少的。从数学来说，施普林格（Springer）出版社至今仍然是世界上最具权威的出版社。科学出版社影印一批他们出版的好的新书，使我国广大数学家能以较低的价格购买，特别是在边远地区工作的数学家能普遍见到这些书，无疑是对推动我国数学的科研与教学十分有益的事。

这次科学出版社购买了版权，一次影印了 23 本施普林格出版社出版的数学书，就是一件好事，也是值得继续做下去的事情。大体上分一下，这 23 本书中，包括基础数学书 5 本，应用数学书 6 本与计算数学书 12 本，其中有些书也具有交叉性质。这些书都是很新的，2000 年以后出版的占绝大部分，共计 16 本，其余的也是 1990 年以后出版的。这些书可以使读者较快地了解数学某方面的前沿，例如基础数学中的数论、代数与拓扑三本，都是由该领域大数学家编著的“数学百科全书”的分册。对从事这方面研究的数学家了解该领域的前沿与全貌很有帮助。按照学科的特点，基础数学类的书以“经典”为主，应用和计算数学类的书以“前沿”为主。这些书的作者多数是国际知名的大数学家，例如《拓扑学》一书的作者诺维科夫是俄罗斯科学院的院士，曾获“菲尔兹奖”和“沃尔夫数学奖”。这些大数学家的著作无疑将会对我国的科研人员起到非常好的指导作用。

当然，23 本书只能涵盖数学的一部分，所以，这项工作还应该继续做下去。更进一步，有些读者面较广的好书还应该翻译成中文出版，使之有更大的读者群。

总之，我对科学出版社影印施普林格出版社的部分数学著作这一举措表示热烈的支持，并盼望这一工作取得更大的成绩。

王　元

2005 年 12 月 3 日

Preface to the Third Edition

After 10 years (or should I say 4000 years?) what's new? Too much to accommodate here, even though we've continued to grow exponentially. Sections **A20, C21, D29** and **F32** have been added, and existing sections expanded. The bibliographies are no doubt one of the more useful aspects of the book, but have become so extensive in some places that occasional reluctant pruning has taken place, leaving the reader to access secondary, but at least more accessible, sources.

A useful new feature is the lists, at the ends of about half of the sections, of references to **OEIS**, Neil Sloane's Online Encyclopedia of Integer Sequences. Many thanks to Neil for his suggestion, and for his help with its implementation. As this is a first appearance, many sequences will be missing that ought to be mentioned, and a few that are may be inappropriately placed. As more people make use of this important resource, I hope that they will let me have a steady stream of further suggestions.

I get a great deal of pleasure from the interest that so many people have shown, and consequently the help that they provide. This happens so often that it is impossible to acknowledge all of it here. Many names are mentioned in earlier prefaces. I especially miss Dick Lehmer, Raphael Robinson and Paul Erdős [the various monetary rewards he offered may still be negotiable via Ron Graham].

Renewed thanks to those mentioned earlier and new or renewed thanks to Stefan Bartels, Mike Bennett, David Boyd, Andrew Bremner, Kevin Brown, Kevin Buzzard, Chris Caldwell, Phil Carmody, Henri Cohen, Karl Dilcher, Noam Elkies, Scott Forrest, Dean Hickerson, Dan Hoey, Dave Hough, Florian Luca, Ronald van Luijk, Greg Martin, Jud McCranie, Pieter Moree, Gerry Myerson, Ed Pegg, Richard Pinch, Peter Pleasants, Carl Pomerance, Randall Rathbun, Herman te Riele, John Robertson, Rainer Rosenthal, Renate Scheidler, Rich Schroeppel, Jamie Simpson, Neil Sloane, Jozsef Solymosi, Cam Stewart, Robert Styer, Eric Weisstein, Hugh Williams, David W. Wilson, Robert G. Wilson, Paul Zimmerman, Rita Zuazua: and apologies to those who are omitted.

A special thankyou to Jean-Martin Albert for resuscitating Andy Guy's programme. I am also grateful to the Natural Sciences & Engineering Research Council of Canada for their ongoing support, and to the Department of Mathematics & Statistics of The University of Calgary for having extended their hospitality twenty-one years after retirement. I look forward to the next twenty-one. And thank you to Springer, and to Ina Lindemann and Mark Spencer in particular, for continuing to maintain excellence in both their finished products and their personal relationships.

Calgary 2003-09-16 Richard K. Guy

Preface to the Second Edition

Erdős recalls that Landau, at the International Congress in Cambridge in 1912, gave a talk about primes and mentioned four problems (see **A1**, **A5**, **C1** below) which were unattackable in the present state of science, and says that they still are. On the other hand, since the first edition of this book, some remarkable progress has been made. Fermat's last theorem (modulo some holes that are expected to be filled in), the Mordell conjecture, the infinitude of Carmichael numbers, and a host of other problems have been settled.

The book is perpetually out of date; not always the 1700 years of one statement in **D1** in the first edition, but at least a few months between yesterday's entries and your reading of the first copies off the press. To ease comparison with the first edition, the numbering of the sections is still the same. Problems which have been largely or completely answered are **B47**, **D2**, **D6**, **D8**, **D16**, **D26**, **D27**, **D28**, **E15**, **F15**, **F17** & **F28**. Related open questions have been appended in some cases, but in others they have become exercises, rather than problems.

Two of the author's many idiosyncrasies are mentioned here: the use of the ampersand (&) to denote joint work and remove any possible ambiguity from phrases such as '... follows from the work of Gauß and Erdős & Guy'; and the use of the notation

¿ . . . . ?

borrowed from the Hungarians, for a conjectural or hypothetical statement. This could have alleviated some anguish had it been used by the well intentioned but not very well advised author of an introductory calculus text. A student was having difficulty in finding the derivative of a product. Frustrated myself, I asked to see the student's text. He had highlighted a displayed formula stating that the derivative of a product was the product of the derivatives, without noting that the context was 'Why is ... not the right answer?'

The threatened volume on *Unsolved Problems in Geometry* has appeared, and is already due for reprinting or for a second edition.

It will be clear from the text how many have accepted my invitation to use this as a clearing house and how indebted I am to correspondents.

Extensive though it is, the following list is far from complete, but I should at least offer my thanks to 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 Erdős, 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 & 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 and Don Zagier. I particularly miss the impeccable proof-reading, the encyclopedic knowledge of the literature, and the clarity and ingenuity of the mathematics of John Leech.

Thanks also to Andy Guy for setting up the electronic framework which has made both the author's and the publisher's task that much easier. The Natural Sciences and Engineering Research Council of Canada continue to support this and many other of the author's projects.

Calgary 94-01-08 Richard K. Guy

Preface to the First Edition

To many laymen, mathematicians appear to be problem solvers, people who do "hard sums". Even inside the profession we classify ourselves as either theorists or problem solvers. Mathematics is kept alive, much more than by the activities of either class, by the appearance of a succession of unsolved problems, both from within mathematics itself and from the increasing number of disciplines where it is applied. Mathematics often owes more to those who ask questions than to those who answer them. The solution of a problem may stifle interest in the area around it. But "Fermat's Last Theorem", because it is not yet a theorem, has generated a great deal of "good" mathematics, whether goodness is judged by beauty, by depth or by applicability.

To pose good unsolved problems is a difficult art. The balance between triviality and hopeless unsolvability is delicate. There are many simply stated problems which experts tell us are unlikely to be solved in the next generation. But we have seen the Four Color Conjecture settled, even if we don't live long enough to learn the status of the Riemann and Goldbach hypotheses, of twin primes or Mersenne primes, or of odd perfect numbers. On the other hand, "unsolved" problems may not be unsolved at all, or may be much more tractable than was at first thought.

Among the many contributions made by Hungarian mathematician Erdős Pál, not least is the steady flow of well-posed problems. As if these were not incentive enough, he offers rewards for the first solution of many of them, at the same time giving his estimate of their difficulty. He has made many payments, from $1.00 to $1000.00.

One purpose of this book is to provide beginning researchers, and others who are more mature, but isolated from adequate mathematical stimulus, with a supply of easily understood, if not easily solved, problems which they can consider in varying depth, and by making occasional partial progress, gradually acquire the interest, confidence and persistence that are essential to successful research.

But the book has a much wider purpose. It is important for students and teachers of mathematics at all levels to realize that although they are not yet capable of research and may have no hopes or ambitions in that direction, there are plenty of unsolved problems that are well within their comprehension, some of which will be solved in their lifetime. Many amateurs have been attracted to the subject and many successful researchers first gained their confidence by examining problems in euclidean geometry, in number theory, and more recently in combinatorics and graph theory, where it is possible to understand questions and even to formulate them and obtain original results without a deep prior theoretical knowledge.

The idea for the book goes back some twenty years, when I was impressed by the circulation of lists of problems by the late Leo Moser and co-author Hallard Croft, and by the articles of Erdős. Croft agreed to let me help him amplify his collection into a book, and Erdős has repeatedly encouraged and prodded us. After some time, the Number Theory chapter swelled into a volume of its own, part of a series which will contain a volume on Geometry, Convexity and Analysis, written by Hallard T. Croft, and one on Combinatorics, Graphs and Games by the present writer.

References, sometimes extensive bibliographies, are collected at the end of each problem or article surveying a group of problems, to save the reader from turning pages. In order not to lose the advantage of having all references collected in one alphabetical list, we give an Index of Authors, from which particular papers can easily be located provided the author is not too prolific. Entries in this index and in the General Index and Glossary of Symbols are to problem numbers instead of page numbers.

Many people have looked at parts of drafts, corresponded and made helpful comments. Some of these were personal friends who are no longer with us: Harold Davenport, Hans Heilbronn, Louis Mordell, Leo Moser, Theodor Motzkin, Alfred Rényi and Paul Turán. Others are H. L. Abbott, J. W. S. Cassels, J. H. Conway, P. Erdős, Martin Gardner, R. L. Graham, H. Halberstam, D. H. and Emma Lehmer, A. M. Odlyzko, Carl Pomerance, A. Schinzel, J. L. Selfridge, N. J. A. Sloane, E. G. Straus, H. P. F. Swinnerton-Dyer and Hugh Williams. A grant from the National Research Council of Canada has facilited contact with these and many others. The award of a Killam Resident Fellowship at the University of Calgary was especially helpful during the writing of a final draft. The technical typing was done by Karen McDermid, by Betty Teare and by Louise Guy, who also helped with the proof-reading. The staff of Springer-Verlag in New York has been courteous, competent and helpful.

In spite of all this help, many errors remain, for which I assume reluctant responsibility. In any case, if the book is to serve its purpose it will start becoming out of date from the moment it appears; it has been becoming out of date ever since its writing began. I would be glad to hear from readers. There must be many solutions and references and problems which I don't know about. I hope that people will avail themselves of this clearing house. A few good researchers thrive by rediscovering results for themselves, but many of us are disappointed when we find that our discoveries have been anticipated.

Calgary 81-08-13 Richard K. Guy

Glossary of Symbols

A.P.	arithmetic progression, $a, a+d, \ldots a+kd, \ldots$.	A5, A6, E10, E33
$a_1 \equiv a_2 \bmod b$	a_1 congruent to a_2, modulo b; $a_1 - a_2$ divisible by b.	A3, A4, A12, A15, B2, B4, B7, ...
$A(x)$	number of members of a sequence not exceeding x; e.g. number of amicable numbers not exceeding x	B4, E1, E2, E4
c	a positive constant (not always the same!)	A1, A3, A8, A12, B4, B11, ...
d_n	difference between consecutive primes; $p_{n+1} - p_n$	A8, A10, A11
$d(n)$	the number of (positive) divisors of n; $\sigma_0(n)$	B, B2, B8, B12, B18, ...
$d \mid n$	d divides n; n is a multiple of d; there is an integer q such that $dq = n$	B, B17, B32, B37, B44, C20, D2, E16
$d \nmid n$	d does not divide n	B, B2, B25, D2, E14, E16, ...
e	base of natural logarithms; 2.718281828459045...	A8, B22, B39, D12, ...
E_n	Euler numbers; coefficients in series for $\sec x$	B45
exp{..}	exponential function	A12, A19, B4, B36, B39, ...
F_n	Fermat numbers; $2^{2^n} + 1$	A3, A12

$f(x) \sim g(x)$	$f(x)/g(x) \to 1$ as $x \to \infty$. (f, $g > 0$)	A1, A3, A8, B33, B41, C1, C17, D7, E2, E30, F26
$f(x) = o(g(x))$	$f(x)/g(x) \to 0$ as $x \to \infty$. ($g > 0$)	A1, A18, A19, B4, C6, C9, C11, C16, C20, D4, D11, E2, E14, F1
$f(x) = O(g(x))$	there is a c such that $\|f(x)\| < cg(x)$ for all sufficiently large x ($g(x) > 0$).	A19, B37, C8, C9, C10, C12, C16, D4, D12, E4, E8, E20, E30, F1, F2, F16
$f(x) \ll g(x)$	(as above)	A4, B4, B18, B32, B40, C9, C14, D11, E28, F4
$f(x) = \Omega(g(x))$	there is a $c > 0$ such that there are arbitrarily large x with $\|f(x)\| \geq cg(x)$ ($g(x) > 0$).	D12, E25
$f(x) \asymp g(x)$	there are c_1, c_2 such that $c_1 g(x) \leq f(x) \leq c_2 g(x)$ ($g(x) > 0$) for all sufficiently large x.	B18
$f(x) = \Theta(g(x))$	(as above)	E20
i	square root of -1; $i^2 = -1$	A16
$\ln x$	natural logarithm of x	A1, A2, A3, A5, A8, A12, ...
(m, n)	g.c.d. (greatest common divisor) of m and n; h.c.f. (highest common factor) of m and n	A, B3, B4, B5 B11, D2
$[m, n]$	l.c.m. (least common multiple) of m and n.	B35, E2, F14
	Also the block of consecutive integers, m, $m+1$, ..., n	B24, B26, B32, C12, C16
$m \perp n$	m, n coprime; $(m, n) = 1$; m prime to n.	A, A4, B3, B4, B5, B11, D2
M_n	Mersenne numbers; $2^n - 1$	A3, B11, B38

$n!$	factorial n; $1 \times 2 \times 3 \times \cdots \times n$	A2, B12, B14, B22 B23, B43, ...
$!n$	$0! + 1! + 2! + \ldots + (n-1)!$	B44
$\binom{n}{k}$	n choose k; the binomial coefficient $n!/k!(n-k)!$	B31, B33, C10, D3
$\left(\frac{p}{q}\right)$	Legendre (or Jacobi) symbol	see F5 (A1, A12, F7)
$p^a \\| n$	p^a divides n, but p^{a+1} does not divide n	B, B8, B37, F16
p_n	the nth prime, $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, ...	A2, A5, A14, A17 E30
$P(n)$	largest prime factor of n	B30, B46
$\mathbb{Q}$	the field of rational numbers	D2, F7
$r_k(n)$	least number of numbers not exceeding n, which must contain a k-term A.P.	see E10
$s(n)$	sum of aliquot parts (divisors of n other than n) of n; $\sigma(n) - n$	B, B1, B2, B8, B10, ...
$s^k(n)$	kth iterate of $s(n)$	B, B6, B7
$s^*(n)$	sum of unitary aliquot parts of n	B8
$S \bigcup T$	union of sets S and T	E7
$W(k,l)$	van der Waerden number	see E10
$\lfloor x \rfloor$	floor of x; greatest integer not greater than x.	A1, A5, C7, C12, C15, ...
$\lceil x \rceil$	ceiling of x; least integer not less than x.	B24
$\mathbb{Z}$	the integers $\ldots, -2, -1, 0, 1, 2, \ldots$	F14
$\mathbb{Z}_n$	the ring of integers, 0, 1, 2, ..., $n-1$ (modulo n)	E8
γ	Euler's constant; 0.577215664901532...	A8

ϵ	arbitrarily small positive constant.	A8, A18, A19, B4, B11, ...
ζ_p	p-th root of unity.	D2
$\zeta(s)$	Riemann zeta-function; $\sum_{n=1}^{\infty}(1/n^s)$	D2
π	ratio of circumference of circle to diameter; 3.141592653589793...	F1, F17
$\pi(x)$	number of primes not exceeding x	A17, E4
$\pi(x; a, b)$	number of primes not exceeding x and congruent to a modulo b	A4
$\prod$	product	A1, A2, A3, A8 A15, ...
$\sigma(n)$	sum of divisors of n; $\sigma_1(n)$	B, B2, B5, B8, B9, ...
$\sigma_k(n)$	sum of kth powers of divisors of n	B, B12, B13, B14
$\sigma^k(n)$	kth iterate of $\sigma(n)$	B9
$\sigma^*(n)$	sum of unitary divisors of n	B8
Σ	sum	A5, A8, A12, B2 B14, ...
$\phi(n)$	Euler's totient function; number of numbers not exceeding n and prime to n	B8, B11, B36, B38, B39, ...
$\phi^k(n)$	kth iterate of $\phi(n)$	B41
ω	complex cube root of 1 $\omega^3 = 1$, $\omega \neq 1$, $\omega^2 + \omega + 1 = 0$	A16
$\omega(n)$	number of distinct prime factors of n	B2, B8, B37
$\Omega(n)$	number of prime factors of n, counting repetitions	B8
¿ $\cdots$?	conjectural or hypothetical statement	A1, A9, B37, C6 E10, E28, F2, F18

Contents