

Gareth A. Jones and J. Mary Jones

Elementary Number Theory

基本数论



Springer

世界图书出版公司

www.wpcbj.com.cn

S

SPRINGER

U

UNDERGRADUATE

M

MATHEMATICS

S

SERIES

Gareth A. Jones and J. Mary Jones

Elementary Number Theory



Springer

图书在版编目 (C I P) 数据

基本数论=Elementary Number Theory: 英文 / (英)
琼斯 (Jones, G. A.) 著. —北京: 世界图书出版公司北
京公司, 2008.5

ISBN 978-7-5062-9228-3

I. 基… II. 琼… III. 数论-英文 IV. 0156

中国版本图书馆CIP数据核字 (2008) 第055588号

书 名: Elementary Number Theory

作 者: Gareth A. Jones & J. Mary Jones

中 译 名: 基本数论

责任编辑: 高蓉 刘慧

出 版 者: 世界图书出版公司北京公司

印 刷 者: 三河国英印务有限公司

发 行: 世界图书出版公司北京公司 (北京朝内大街 137 号 100010)

联系电话: 010-64015659

电子信箱: kjsk@vip.sina.com

开 本: 24开

印 张: 13.5

版 次: 2008 年 05 月第 1 次印刷

版权登记: 图字:01-2008-2093

书 号: 978-7-5062-9228-3 / O · 619

定 价: 46.00 元

世界图书出版公司北京公司已获得 Springer 授权在中国大陆独家重印发行

Springer Undergraduate Mathematics Series

Advisory Board

M.A.J. Chaplain *University of Dundee*
K. Erdmann *Oxford University*
A. MacIntyre *Queen Mary, University of London*
L.C.G. Rogers *University of Cambridge*
E. Süli *Oxford University*
J.F. Toland *University of Bath*

Other books in this series

A First Course in Discrete Mathematics *I. Anderson*
Analytic Methods for Partial Differential Equations *G. Evans, J. Blackledge, P. Yardley*
Applied Geometry for Computer Graphics and CAD, Second Edition *D. Marsh*
Basic Linear Algebra, Second Edition *T.S. Blyth and E.F. Robertson*
Basic Stochastic Processes *Z. Brzeźniak and T. Zastawniak*
Calculus of One Variable *K.E. Hirst*
Complex Analysis *J.M. Howie*
Elementary Differential Geometry *A. Pressley*
Elementary Number Theory *G.A. Jones and J.M. Jones*
Elements of Abstract Analysis *M. Ó Searcóid*
Elements of Logic via Numbers and Sets *D.L. Johnson*
Essential Mathematical Biology *N.F. Britton*
Essential Topology *M.D. Crossley*
Fields and Galois Theory *J.M. Howie*
Fields, Flows and Waves: An Introduction to Continuum Models *D.F. Parker*
Further Linear Algebra *T.S. Blyth and E.F. Robertson*
Game Theory: Decisions, Interaction and Evolution *J.N. Webb*
General Relativity *N.M.J. Woodhouse*
Geometry *R. Fenn*
Groups, Rings and Fields *D.A.R. Wallace*
Hyperbolic Geometry, Second Edition *J.W. Anderson*
Information and Coding Theory *G.A. Jones and J.M. Jones*
Introduction to Laplace Transforms and Fourier Series *P.P.G. Dyke*
Introduction to Lie Algebras *K. Erdmann and M.J. Wildon*
Introduction to Ring Theory *P.M. Cohn*
Introductory Mathematics: Algebra and Analysis *G. Smith*
Linear Functional Analysis *B.P. Rynne and M.A. Youngson*
Mathematics for Finance: An Introduction to Financial Engineering *M. Capiński and T. Zastawniak*
Metric Spaces *M. Ó Searcóid*
Matrix Groups: An Introduction to Lie Group Theory *A. Baker*
Measure, Integral and Probability, Second Edition *M. Capiński and E. Kopp*
Multivariate Calculus and Geometry, Second Edition *S. Dineen*
Numerical Methods for Partial Differential Equations *G. Evans, J. Blackledge, P. Yardley*
Probability Models *J. Haigh*
Real Analysis *J.M. Howie*
Sets, Logic and Categories *P. Cameron*
Special Relativity *N.M.J. Woodhouse*
Symmetries *D.L. Johnson*
Topics in Group Theory *G. Smith and O. Tabachnikova*
Vector Calculus *P.C. Matthews*
Worlds Out of Nothing: A Course in the History of Geometry in the 19th Century *J. Gray*

Gareth A. Jones, MA, DPhil
School of Mathematics, University of Southampton, Highfield, Southampton,
SO17 1BJ, UK

J. Mary Jones, MA, DPhil
The Open University, Walton Hall, Milton Keynes, MK7 6AA, UK

Cover illustration elements reproduced by kind permission of

Aptech Systems, Inc., Publishers of the GAUSS Mathematical and Statistical System, 23804 S.E. Kent-Kangley Road, Maple Valley, WA 98038,
USA. Tel (206) 432 - 7855 Fax (206) 432 - 7832 email: info@aptech.com URL: www.aptech.com

American Statistical Association: Chance Vol 8 No 1, 1995 article by KS and KW Heiner 'Tree Rings of the Northern Shawangunks' page 32 fig 2

Springer-Verlag: *Mathematica in Education and Research* Vol 4 Issue 3 1995 article by Roman E Maeder, Beatrice Amrhein and Oliver Gloor
'Illustrated Mathematics: Visualization of Mathematical Objects' page 9 fig 11, originally published as a CD ROM 'Illustrated Mathematics' by
TELOS: ISBN 0-387-14222-3, German edition by Birkhauser: ISBN 3-7643-5100-4.

Mathematica in Education and Research Vol 4 Issue 3 1995 article by Richard J Gaylord and Kazume Nishidate 'Traffic Engineering with Cellular
Automata' page 35 fig 2. *Mathematica in Education and Research* Vol 5 Issue 2 1996 article by Michael Trott 'The Implicitization of a Trefoil
Knot' page 14.

Mathematica in Education and Research Vol 5 Issue 2 1996 article by Lee de Cola 'Coins, Trees, Bars and Bells: Simulation of the Binomial Process'
page 19 fig 3. *Mathematica in Education and Research* Vol 5 Issue 2 1996 article by Richard Gaylord and Kazume Nishidate 'Contagious
Spreading' page 33 fig 1. *Mathematica in Education and Research* Vol 5 Issue 2 1996 article by Joe Buhler and Stan Wagon 'Secrets of the
Machung Constant' page 50 fig 1.

British Library Cataloguing in Publication Data

Jones, Gareth A.

Elementary number theory. - (Springer undergraduate mathematics series)

1. Number theory

I. Title II. Jones, J. Mary

512.7'2

ISBN 3540761977

Library of Congress Cataloging-in-Publication Data

Jones, Gareth A.

Elementary number theory / Gareth A. Jones and J. Mary Jones.

p. cm. -- (Springer undergraduate mathematics series)

Includes bibliographical references and index.

ISBN 3-540-76197-7 (pbk.: alk. paper)

1. Number theory. I. Jones, J. Mary (Josephine Mary), 1946-

II. Title. III. Series.

QA241. J62 1998

97-41193

512'.7—dc21

CIP

Apart from any fair dealing for the purposes of research or private study, or criticism or review, as permitted under the Copyright, Designs and Patents Act 1988, this publication may only be reproduced, stored or transmitted, in any form or by any means, with the prior permission in writing of the publishers, or in the case of reprographic reproduction in accordance with the terms of licences issued by the Copyright Licensing Agency. Enquiries concerning reproduction outside those terms should be sent to the publishers.

Springer Undergraduate Mathematics Series ISSN 1615-2085

ISBN 3-540-76197-7

Springer Science+Business Media

springer.com

© Springer-Verlag London Limited 1998

10th printing 2006

The use of registered names, trademarks etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant laws and regulations and therefore free for general use.

The publisher makes no representation, express or implied, with regard to the accuracy of the information contained in this book and cannot accept any legal responsibility or liability for any errors or omissions that may be made.

This reprint has been authorized by Springer-Verlag (Berlin/Heidelberg/New York) for sale in the People's Republic of China only and not for export therefrom.

Preface

Our intention in writing this book is to give an elementary introduction to number theory which does not demand a great deal of mathematical background or maturity from the reader, and which can be read and understood with no extra assistance. Our first three chapters are based almost entirely on A-level mathematics, while the next five require little else beyond some elementary group theory. It is only in the last three chapters, where we treat more advanced topics, including recent developments, that we require greater mathematical background; here we use some basic ideas which students would expect to meet in the first year or so of a typical undergraduate course in mathematics. Throughout the book, we have attempted to explain our arguments as fully and as clearly as possible, with plenty of worked examples and with outline solutions for all the exercises.

There are several good reasons for choosing number theory as a subject. It has a long and interesting history, ranging from the earliest recorded times to the present day (see Chapter 11, for instance, on Fermat's Last Theorem), and its problems have attracted many of the greatest mathematicians; consequently the study of number theory is an excellent introduction to the development and achievements of mathematics (and, indeed, some of its failures). In particular, the explicit nature of many of its problems, concerning basic properties of integers, makes number theory a particularly suitable subject in which to present modern mathematics in elementary terms.

A second reason is that many students nowadays are unfamiliar with the notion of formal proof; this is best taught in a concrete setting, rather than as an abstract exercise in logic, but earlier choices of context, such as geometry and analysis, have suffered from the conceptual difficulty and abstract nature of their subject-matter, whereas number theory is about very familiar and easily manipulated objects, namely integers. We therefore see this book as a vehicle for

explaining how mathematicians go about their business, finding experimental evidence, making conjectures, creating proofs and counterexamples, and so on.

A third reason is that many students prefer computation to abstraction, and number theory, with its discrete, precise nature, is an ideal topic in which to perform numerical experiments and calculations. Many of these can be done by hand, and throughout the book we have given examples and exercises of an algorithmic nature. Nowadays, almost every student has access to computing facilities far in excess of anything the great calculator Gauss could have imagined, and for a few of our exercises such electronic assistance is desirable or even essential. We have not linked our approach to any particular machine, programming language or computer algebra system, since even a fairly primitive pocket calculator or personal computer can greatly enhance one's ability to do number theory (and part of the fun lies in persuading it to do so).

A final reason for learning number theory is that, despite Hardy's (1940) famous but now out-dated claim, it is useful. Its best-known modern application is to the cryptographic systems which allow banks, commercial companies, military establishments, and so on to exchange information in securely-encoded form; many of these systems are based on such number-theoretic properties as the apparent difficulty of factorising very large integers (see Chapters 2 and 5). Physicists, engineers and computer scientists are also finding that number-theoretic concepts are playing an increasing role in their work. These applications were not the original motivation for the great developments in number theory, but their emergence can only add to the importance of the subject.

The first three chapters of this book are intended to be accessible to anyone with a little A-level mathematics. In particular, they are suitable for first-year university students and for the more advanced sixth-formers. Equivalence relations appear in Chapter 3, but otherwise no abstract mathematics is used. Proof by induction is used several times, and three versions of this (including strong induction and the well-ordering principle) are summarised in Appendix A. Chapters 4–8 are a little more algebraic in flavour, and require slightly greater mathematical maturity. Here, it is helpful if the reader has met some elementary group theory (subgroups, cyclic groups, direct products, isomorphisms), and knows what rings and fields are; these topics are summarised in Appendix B. Probabilities are also mentioned, though not in any essential way. These chapters are therefore suitable for second- or third-year students, and also for those first-year students sufficiently interested to want to read further. The last three chapters are more advanced, relying on ideas from other areas of mathematics such as analysis, calculus, geometry and algebra which students will almost certainly have met early in their undergraduate studies; these include convergence (summarised in Appendix C), power series, complex numbers and vector spaces. These chapters should therefore be suitable for

students at second- or third-year level. The final chapter, which traces Fermat's Last Theorem from its ancient roots to its recent proof, is rather more descriptive and historical in style than the others, but we have tried to include sufficient technical detail to give the reader a flavour of this exciting topic.

The early parts of the book could be used as a first-year introduction to the concepts and methods of pure mathematics, while the rest could form the basis for a more specialised second- or third-year course in number theory. Indeed, many of the chapters are based on courses we have taught to first- and third-year mathematics students at the University of Southampton. The book is also suitable for other students, such as computer scientists and physicists, who want an elementary introduction which brings them up to date with recent developments in the subject.

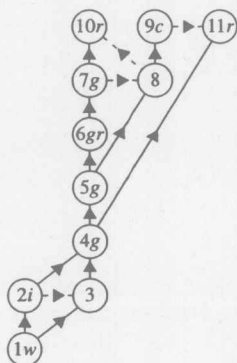
The two essentials for starting number theory are confidence with traditional algebraic manipulation, and some conception of formal proof. Unfortunately, the recent expansion of university education in the UK has coincided with a decline in numbers taking Further Mathematics A-level, so mathematics students now arrive at university much less familiar with these topics than their predecessors were. In our first few chapters we have therefore taken a more leisurely approach than is traditional, using simple results in number theory to illustrate methods of proof, and emphasising algorithmic and computational aspects in parallel with theory. In later chapters, the pace is rather brisker, but even here we have attempted to present our arguments in as simple terms as possible in order to make them more widely accessible. In the case of some advanced results, this has forced us to concentrate on special cases, or to give only outline proofs, but we think this is a worthwhile sacrifice if it conveys to our readers some feeling of what high-level mathematics is like and how it is done – too many mathematics students graduate with only the vaguest idea of the great problems and achievements of their subject.

We would like to thank Peter Neumann for showing us how to discover and communicate mathematics, and many of our colleagues at Southampton, especially Ann and Keith Hirst and David Singerman, for their sound advice on teaching mathematics in general and number theory in particular. We are very grateful to Susan Hezlet and her colleagues at Springer for their advice and encouragement. It is also traditional to thank one's partner for patience and tolerance during the preparation of a book; instead, we shall simply thank our children for not playing their music any louder than was absolutely necessary.

Notes to the Reader

Mathematics is a difficult subject to read, and number theory is no exception, even if its subject matter is less abstract than some other topics. Do not be surprised, therefore, if it takes you several attempts before you completely understand an argument. It is often useful when reading mathematics to make notes and to do calculations as you go along; for instance, a general argument can often be clarified by seeing how it works in some specific cases.

Exercises are an important part of the learning process, and you are encouraged to attempt them while reading each section; we have generally placed them immediately after the topics on which they are based, to reinforce your understanding of those topics. Supplementary exercises, which are generally more demanding, are placed at the end of a chapter; they can refer to anything in that chapter, and possibly also to topics covered in earlier chapters. Answers or outline solutions for all the exercises are given at the end of the book; how-



ever, there is a great deal more to be gained from trying the exercises first, before reading the solutions!

The diagram on page xiii shows the interdependence of chapters, with continuous and broken lines indicating strong and weak links. Thus, to understand Chapter 11 it is sufficient to have read Chapters 1–4, though it also helps to know a little of the material in Chapter 9. The letters *i* and *w* indicate that the principles of induction and well-ordering are used; these are summarised in Appendix A. Similarly *g* and *r* refer to material on groups and rings (Appendix B), and *c* to convergence (Appendix C).



Contents

Notes to the Reader	xiii
1. Divisibility	1
1.1 Divisors	2
1.2 Bezout's identity	7
1.3 Least common multiples	12
1.4 Linear Diophantine equations	13
1.5 Supplementary exercises	16
2. Prime Numbers	19
2.1 Prime numbers and prime-power factorisations	19
2.2 Distribution of primes	25
2.3 Fermat and Mersenne primes	30
2.4 Primality-testing and factorisation	32
2.5 Supplementary exercises	35
3. Congruences	37
3.1 Modular arithmetic	37
3.2 Linear congruences	46
3.3 Simultaneous linear congruences	52
3.4 Simultaneous non-linear congruences	57
3.5 An extension of the Chinese Remainder Theorem	59
3.6 Supplementary exercises	62
4. Congruences with a Prime-power Modulus	65
4.1 The arithmetic of \mathbb{Z}_p	65
4.2 Pseudoprimes and Carmichael numbers	72

4.3	Solving congruences mod (p^e)	78
4.4	Supplementary exercises	82
5.	Euler's Function	83
5.1	Units	83
5.2	Euler's function	85
5.3	Applications of Euler's function	92
5.4	Supplementary exercises	96
6.	The Group of Units	97
6.1	The group U_n	97
6.2	Primitive roots	99
6.3	The group U_{p^e} , where p is an odd prime	103
6.4	The group U_{2^e}	106
6.5	The existence of primitive roots	108
6.6	Applications of primitive roots	110
6.7	The algebraic structure of U_n	113
6.8	The universal exponent	116
6.9	Supplementary exercises	117
7.	Quadratic Residues	119
7.1	Quadratic congruences	119
7.2	The group of quadratic residues	120
7.3	The Legendre symbol	123
7.4	Quadratic reciprocity	130
7.5	Quadratic residues for prime-power moduli	135
7.6	Quadratic residues for arbitrary moduli	138
7.7	Supplementary exercises	140
8.	Arithmetic Functions	143
8.1	Definition and examples	143
8.2	Perfect numbers	146
8.3	The Möbius Inversion Formula	148
8.4	An application of the Möbius Inversion Formula	152
8.5	Properties of the Möbius function	154
8.6	The Dirichlet product	157
8.7	Supplementary exercises	162
9.	The Riemann Zeta Function	163
9.1	Historical background	163
9.2	Convergence	165
9.3	Applications to prime numbers	166

9.4	Random integers	170
9.5	Evaluating $\zeta(2)$	174
9.6	Evaluating $\zeta(2k)$	176
9.7	Dirichlet series	179
9.8	Euler products	182
9.9	Complex variables	185
9.10	Supplementary exercises	188
10.	Sums of Squares	191
10.1	Sums of two squares	191
10.2	The Gaussian integers	196
10.3	Sums of three squares	201
10.4	Sums of four squares	202
10.5	Digression on quaternions	205
10.6	Minkowski's Theorem	206
10.7	Supplementary exercises	214
11.	Fermat's Last Theorem	217
11.1	The problem	217
11.2	Pythagoras's Theorem	218
11.3	Pythagorean triples	219
11.4	Isosceles triangles and irrationality	221
11.5	The classification of Pythagorean triples	223
11.6	Fermat	226
11.7	The case $n = 4$	227
11.8	Odd prime exponents	228
11.9	Lamé and Kummer	233
11.10	Modern developments	234
11.11	Further reading	237
	Appendix A. Induction and Well-ordering	239
	Appendix B. Groups, Rings and Fields	243
	Appendix C. Convergence	247
	Appendix D. Table of Primes $p < 1000$	249
	Solutions to Exercises	251
	Bibliography	289
	Index of symbols	291

1

Divisibility

We start with a number of fairly elementary results and techniques, mainly about greatest common divisors. You have probably met some of this material already, though it may not have been treated as formally as here. There are several good reasons for giving very precise definitions and proofs, even when there is general agreement about the validity of the mathematics involved. The first is that 'general agreement' is not the same as convincing proof: it is not unknown for majority opinion to be seriously mistaken about some point. A second reason is that, if we know exactly what assumptions are required in order to deduce certain conclusions, then we may be able to deduce similar conclusions in other areas where the same assumptions hold true. For example, this chapter is entirely devoted to the divisibility properties of *integers*, but it turns out that very similar definitions, methods and theorems are valid for certain other objects which can be added, subtracted and multiplied; some of these objects, such as polynomials, are very familiar, while others, such as Gaussian integers and quaternions, will be introduced in later chapters. These generalisations of the integers are also explored in algebra, under the heading of ring theory.

1.1 Divisors

Our starting-point is the *division algorithm*, which is as follows:

Theorem 1.1

If a and b are integers with $b > 0$, then there is a unique pair of integers q and r such that

$$a = qb + r \quad \text{and} \quad 0 \leq r < b.$$

Example 1.1

If $a = 9$ and $b = 4$ then we have $9 = 2 \times 4 + 1$ with $0 \leq 1 < 4$, so $q = 2$ and $r = 1$; if $a = -9$ and $b = 4$ then $q = -3$ and $r = 3$.

In Theorem 1.1, we call q the *quotient* and r the *remainder*. By dividing by b , so that

$$\frac{a}{b} = q + \frac{r}{b} \quad \text{and} \quad 0 \leq \frac{r}{b} < 1,$$

we see that q is the integer part $\lfloor a/b \rfloor$ of a/b , the greatest integer $i \leq a/b$. This makes it easy to calculate q , and then to find $r = a - qb$.

Proof

First we prove existence. Let

$$S = \{a - nb \mid n \in \mathbb{Z}\} = \{a, a \pm b, a \pm 2b, \dots\}.$$

This set of integers contains non-negative elements (take $n = -\lfloor a/b \rfloor$), so $S \cap \mathbb{N}$ is a non-empty subset of \mathbb{N} ; by the well-ordering principle (see Appendix A), $S \cap \mathbb{N}$ has a least element, which has the form $r = a - qb \geq 0$ for some integer q . Thus $a = qb + r$ with $r \geq 0$. If $r \geq b$ then S contains a non-negative element $a - (q+1)b = r - b < r$; this contradicts the minimality of r , so we must have $r < b$.

To prove uniqueness, suppose that $a = qb + r = q'b + r'$ with $0 \leq r < b$ and $0 \leq r' < b$, so $r - r' = (q' - q)b$. If $q' \neq q$ then $|q' - q| \geq 1$, so $|r - r'| \geq |b| = b$, which is impossible since r and r' lie between 0 and $b-1$ inclusive. Hence $q' = q$ and so $r' = r$. \square

We can now deal with the case $b < 0$: since $-b > 0$, Theorem 1.1 implies that there exist integers q^* and r such that $a = q^*(-b) + r$ and $0 \leq r < -b$, so