

DISCRETE MATHEMATICS AND ITS APPLICATIONS
Series Editor KENNETH H. ROSEN

DIOPHANTINE ANALYSIS

JÖRN STEUDING

 Chapman & Hall/CRC
Taylor & Francis Group
Boca Raton London New York Singapore

CRC Press
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

© 2005 by Taylor & Francis Group, LLC
CRC Press is an imprint of Taylor & Francis Group, an Informa business

No claim to original U.S. Government works
Version Date: 20110713

International Standard Book Number-13: 978-1-4200-5720-1 (eBook - PDF)

This book contains information obtained from authentic and highly regarded sources. Reasonable efforts have been made to publish reliable data and information, but the author and publisher cannot assume responsibility for the validity of all materials or the consequences of their use. The authors and publishers have attempted to trace the copyright holders of all material reproduced in this publication and apologize to copyright holders if permission to publish in this form has not been obtained. If any copyright material has not been acknowledged please write and let us know so we may rectify in any future reprint.

Except as permitted under U.S. Copyright Law, no part of this book may be reprinted, reproduced, transmitted, or utilized in any form by any electronic, mechanical, or other means, now known or hereafter invented, including photocopying, microfilming, and recording, or in any information storage or retrieval system, without written permission from the publishers.

For permission to photocopy or use material electronically from this work, please access www.copyright.com (<http://www.copyright.com/>) or contact the Copyright Clearance Center, Inc. (CCC), 222 Rosewood Drive, Danvers, MA 01923, 978-750-8400. CCC is a not-for-profit organization that provides licenses and registration for a variety of users. For organizations that have been granted a photocopy license by the CCC, a separate system of payment has been arranged.

Trademark Notice: Product or corporate names may be trademarks or registered trademarks, and are used only for identification and explanation without intent to infringe.

Visit the Taylor & Francis Web site at
<http://www.taylorandfrancis.com>

and the CRC Press Web site at
<http://www.crcpress.com>

Contents

Preface

Chapter 1. Introduction: basic principles	
1.1. Who was Diophantus?	1
1.2. Pythagorean triples	2
1.3. Fermat's last theorem	3
1.4. The method of infinite descent	4
1.5. Cantor's paradise	6
1.6. Irrationality of e	7
1.7. Irrationality of π	8
1.8. Approximating with rationals	10
1.9. Linear diophantine equations	12
Exercises	14
Chapter 2. Classical approximation theorems	
2.1. Dirichlet's approximation theorem	17
2.2. A first irrationality criterion	19
2.3. The order of approximation	19
2.4. Kronecker's approximation theorem	21
2.5. Billiard	22
2.6. Uniform distribution	23
2.7. The Farey sequence	25
2.8. Mediants and Ford circles	26
2.9. Hurwitz' theorem	28
2.10. Padé approximation	30
Exercises	32
Chapter 3. Continued fractions	
3.1. The Euclidean algorithm revisited and calendars	36
3.2. Finite continued fractions	37
3.3. Interlude: Egyptian fractions	39
3.4. Infinite continued fractions	42
3.5. Approximating with convergents	43
3.6. The law of best approximations	44
3.7. Consecutive convergents	45
3.8. The continued fraction for e	46
Exercises	49

Chapter 4. The irrationality of $\zeta(3)$	
4.1. The Riemann zeta-function	52
4.2. Apéry's theorem	54
4.3. Approximating $\zeta(3)$	54
4.4. A recursion formula	56
4.5. The speed of convergence	58
4.6. Final steps in the proof	60
4.7. An irrationality measure	62
4.8. A non-simple continued fraction	63
4.9. Beukers' proof	64
Notes on recent results	66
Exercises	66
Chapter 5. Quadratic irrationals	
5.1. Fibonacci numbers and paper folding	71
5.2. Periodic continued fractions	73
5.3. Galois' theorem	75
5.4. Square roots	77
5.5. Equivalent numbers	78
5.6. Serret's theorem	79
5.7. The Markoff spectrum	80
5.8. Badly approximable numbers	82
Notes on the metric theory	82
Exercises	84
Chapter 6. The Pell equation	
6.1. The cattle problem	88
6.2. Lattice points on hyperbolas	90
6.3. An infinitude of solutions	92
6.4. The minimal solution	94
6.5. The group of solutions	95
6.6. The minus equation	96
6.7. The polynomial Pell equation	97
6.8. Nathanson's theorem	100
Notes for further reading	102
Exercises	103
Chapter 7. Factoring with continued fractions	
7.1. The RSA cryptosystem	107
7.2. A diophantine attack on RSA	109
7.3. An old idea of Fermat	110
7.4. CFRAC	112
7.5. Examples of failures	115
7.6. Weighted mediants and a refinement	115
Notes on primality testing	117
Exercises	118

Chapter 8. Geometry of numbers	
8.1. Minkowski's convex body theorem	120
8.2. General lattices	122
8.3. The lattice basis theorem	124
8.4. Sums of squares	125
8.5. Applications to linear and quadratic forms	128
8.6. The shortest lattice vector problem	129
8.7. Gram–Schmidt and consequences	131
8.8. Lattice reduction in higher dimensions	132
8.9. The LLL-algorithm	134
8.10. The small integer problem	136
Notes on sphere packings	136
Exercises	137
Chapter 9. Transcendental numbers	
9.1. Algebraic vs. transcendental	141
9.2. Liouville's theorem	142
9.3. Liouville numbers	144
9.4. The transcendence of e	145
9.5. The transcendence of π	147
9.6. Squaring the circle?	149
Notes on transcendental numbers	151
Exercises	152
Chapter 10. The theorem of Roth	
10.1. Roth's theorem	155
10.2. Thue equations	156
10.3. Finite vs. infinite	158
10.4. Differential operators and indices	160
10.5. Outline of Roth's method	162
10.6. Siegel's lemma	164
10.7. The index theorem	165
10.8. Wronskians and Roth's lemma	167
10.9. Final steps in Roth's proof	171
Notes for further reading	173
Exercises	174
Chapter 11. The abc -conjecture	
11.1. Hilbert's tenth problem	177
11.2. The ABC -theorem for polynomials	179
11.3. Fermat's last theorem for polynomials	181
11.4. The polynomial Pell equation revisited	182
11.5. The abc -conjecture	183
11.6. LLL & abc	184
11.7. The Erdős–Woods conjecture	186
11.8. Fermat, Catalan & co.	187
11.9. Mordell's conjecture	189

Notes on <i>abc</i>	190
Exercises	192
Chapter 12. p -adic numbers	
12.1. Non-Archimedean valuations	195
12.2. Ultrametric topology	196
12.3. Ostrowski's theorem	198
12.4. Curious convergence	200
12.5. Characterizing rationals	201
12.6. Completions of the rationals	203
12.7. p -adic numbers as power series	205
12.8. Error-free computing	206
Notes on the p -adic interpolation of the zeta-function	207
Exercises	208
Chapter 13. Hensel's lemma and applications	
13.1. p -adic integers	213
13.2. Solving equations in p -adic numbers	214
13.3. Hensel's lemma	216
13.4. Units and squares	218
13.5. Roots of unity	219
13.6. Hensel's lemma revisited	220
13.7. Hensel lifting: factoring polynomials	221
Notes on p -adics: what we leave out	224
Exercises	224
Chapter 14. The local–global principle	
14.1. One for all and all for one	227
14.2. The theorem of Hasse–Minkowski	228
14.3. Ternary quadratics	229
14.4. The theorems of Chevalley and Warning	232
14.5. Applications and limitations	234
14.6. The local Fermat problem	236
Exercises	237
Appendix A. Algebra and number theory	
A.1. Groups, rings, and fields	239
A.2. Prime numbers	241
A.3. Riemann's hypothesis	242
A.4. Modular arithmetic	243
A.5. Quadratic residues	245
A.6. Polynomials	246
A.7. Algebraic number fields	247
A.8. Kummer's work on Fermat's last theorem	249
Bibliography	251
Index	258