

---

# NUMBER THEORY

An Introduction to Mathematics: Part A

By

WILLIAM A. COPPEL

 Springer

Library of Congress Control Number: 2005934653

*PART A*

ISBN-10: 0-387-29851-7 e-ISBN: 0-387-29852-5

ISBN-13: 978-0387-29851-1

*PART B*

ISBN-10: 0-387-29853-3 e-ISBN: 0-387-29854-1

ISBN-13: 978-0387-29853-5

*2-VOLUME SET*

ISBN-10: 0-387-30019-8 e-ISBN: 0-387-30529-7

ISBN-13: 978-0387-30019-1

Printed on acid-free paper.

---

AMS Subject Classifications: 11-xx, 05B20, 33E05

---

© 2006 Springer Science+Business Media, Inc.

All rights reserved. This work may not be translated or copied in whole or in part without the written permission of the publisher (Springer Science+Business Media, Inc., 233 Spring Street, New York, NY 10013, USA), except for brief excerpts in connection with reviews or scholarly analysis. Use in connection with any form of information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed is forbidden.

The use in this publication of trade names, trademarks, service marks, and similar terms, even if they are not identified as such, is not to be taken as an expression of opinion as to whether or not they are subject to proprietary rights.

Printed in the United States of America.

9 8 7 6 5 4 3 2 1

springeronline.com

# Contents

## Part A

### Preface

<b>I</b>	<b>The expanding universe of numbers</b>	<b>1</b>
0	Sets, relations and mappings	1
1	Natural numbers	5
2	Integers and rational numbers	12
3	Real numbers	21
4	Metric spaces	32
5	Complex numbers	45
6	Quaternions and octonions	56
7	Groups	63
8	Rings and fields	70
9	Vector spaces and associative algebras	74
10	Inner product spaces	82
11	Further remarks	87
12	Selected references	92
<b>II</b>	<b>Divisibility</b>	<b>97</b>
1	Greatest common divisors	97
2	The Bézout identity	105
3	Polynomials	112
4	Euclidean domains	121
5	Congruences	124
6	Sums of squares	138
7	Further remarks	144
8	Selected references	147

<b>III</b>	<b>More on divisibility</b>	<b>151</b>
1	The law of quadratic reciprocity	151
2	Quadratic fields	163
3	Multiplicative functions	176
4	Linear Diophantine equations	185
5	Further remarks	200
6	Selected references	203
<b>IV</b>	<b>Continued fractions and their uses</b>	<b>209</b>
1	The continued fraction algorithm	209
2	Diophantine approximation	216
3	Periodic continued fractions	222
4	Quadratic Diophantine equations	227
5	The modular group	234
6	Non-Euclidean geometry	241
7	Complements	245
8	Further remarks	252
9	Selected references	255
<b>V</b>	<b>Hadamard's determinant problem</b>	<b>261</b>
1	What is a determinant?	261
2	Hadamard matrices	268
3	The art of weighing	273
4	Some matrix theory	276
5	Application to Hadamard's determinant problem	284
6	Designs	288
7	Groups and codes	293
8	Further remarks	299
9	Selected references	301

<b>VI</b>	<b>Hensel's <math>p</math>-adic numbers</b>	<b>305</b>
1	Valued fields	305
2	Equivalence	309
3	Completions	313
4	Non-archimedean valued fields	318
5	Hensel's lemma	324
6	Locally compact valued fields	332
7	Further remarks	338
8	Selected references	338
	<b>Notations</b>	<b>A 1</b>
	<b>Axioms</b>	<b>A 6</b>
	<b>Index</b>	<b>A 7</b>
<b>Part B</b>		
<b>VII</b>	<b>The arithmetic of quadratic forms</b>	<b>341</b>
1	Quadratic spaces	341
2	The Hilbert symbol	355
3	The Hasse–Minkowski theorem	366
4	Supplements	377
5	Further remarks	379
6	Selected references	381
<b>VIII</b>	<b>The geometry of numbers</b>	<b>385</b>
1	Minkowski's lattice point theorem	385
2	Lattices	388
3	Proof of the lattice-point theorem, and some generalizations	393
4	Voronoi cells	401
5	Densest packings	407
6	Mahler's compactness theorem	412
7	Further remarks	419
8	Selected references	422

<b>IX</b>	<b>The number of prime numbers</b>	<b>427</b>
	1 Finding the problem	427
	2 Chebyshev's functions	431
	3 Proof of the prime number theorem	434
	4 The Riemann hypothesis	440
	5 Generalizations and analogues	447
	6 Alternative formulations	452
	7 Some further problems	455
	8 Further remarks	457
	9 Selected references	459
<b>X</b>	<b>A character study</b>	<b>465</b>
	1 Primes in arithmetic progressions	465
	2 Characters of finite abelian groups	466
	3 Proof of the prime number theorem for arithmetic progressions	469
	4 Representations of arbitrary finite groups	476
	5 Characters of arbitrary finite groups	480
	6 Induced representations and examples	486
	7 Applications	493
	8 Generalizations	501
	9 Further remarks	513
	10 Selected references	515
<b>XI</b>	<b>Uniform distribution and ergodic theory</b>	<b>519</b>
	1 Uniform distribution	519
	2 Discrepancy	531
	3 Birkhoff's ergodic theorem	537
	4 Applications	543
	5 Recurrence	556
	6 Further remarks	562
	7 Selected references	564

<b>XII</b>	<b>Elliptic functions</b>	<b>569</b>
1	Elliptic integrals	569
2	The arithmetic-geometric mean	578
3	Elliptic functions	585
4	Theta functions	594
5	Jacobian elliptic functions	602
6	The modular function	608
7	Further remarks	613
8	Selected references	617
<b>XIII</b>	<b>Connections with number theory</b>	<b>621</b>
1	Sums of squares	621
2	Partitions	624
3	Cubic curves	628
4	Mordell's theorem	639
5	Further results and conjectures	651
6	Some applications	657
7	Further remarks	664
8	Selected references	667
	<b>Notations</b>	<b>1</b>
	<b>Axioms</b>	<b>6</b>
	<b>Index</b>	<b>7</b>