For centuries, number theorists have refined their intuition by computing examples. The advent of computers and (especially) sophisticated algorithms has gradually led to the emergence of algorithmic number theory as a distinct field. This young discipline has been shaped by strong connections to computer science, cryptography, and other parts of mathematics. One of its charms is that mathematical ideas often lead to better algorithms. Another striking feature is that the algorithmic worldview has led to fascinating new mathematical ideas and questions.

This volume contains twenty survey articles on topics in algorithmic number theory, written by leading experts in the field. The first two are introductory, aiming to entice the reader into pursuing the subject more deeply. The next eight cover core areas of the field: factoring, primality, smooth numbers, lattices, elliptic curves, algebraic number theory, and fast arithmetic algorithms. The remaining ten articles survey specific topics, often with a distinctive perspective, including cryptography, Arakelov class groups, computational class field theory, zeta functions over finite fields, arithmetic geometry, and modular forms.

Mathematical Sciences Research Institute
Publications

44

Algorithmic Number Theory

Mathematical Sciences Research Institute Publications

1 Freed/Uhlenbeck: *Instantons and Four-Manifolds*, second edition
2 Chern (ed.): *Seminar on Nonlinear Partial Differential Equations*
3 Lepowsky/Mandelstam/Singer (eds.): *Vertex Operators in Mathematics and Physics*
4 Kac (ed.): *Infinite Dimensional Groups with Applications*
5 Blackadar: *K-Theory for Operator Algebras*, second edition
6 Moore (ed.): *Group Representations, Ergodic Theory, Operator Algebras, and Mathematical Physics*
7 Chorin/Majda (eds.): *Wave Motion: Theory, Modelling, and Computation*
8 Gersten (ed.): *Essays in Group Theory*
9 Moore/Schochet: *Global Analysis on Foliated Spaces*, second edition
10–11 Drasin/Earle/Gehring/Kra/Marden (eds.): *Holomorphic Functions and Moduli*
12–13 Ni/Peletier/Serrin (eds.): *Nonlinear Diffusion Equations and Their Equilibrium States*
14 Goodman/de la Harpe/Jones: *Coxeter Graphs and Towers of Algebras*
15 Hochster/Huneke/Sally (eds.): *Commutative Algebra*
16 Ihara/Ribet/Serre (eds.): *Galois Groups over* $\mathbb{Q}$
17 Concus/Finn/Hoffman (eds.): *Geometric Analysis and Computer Graphics*
18 Bryant/Chern/Gardner/Goldschmidt/Griffiths: *Exterior Differential Systems*
19 Alperin (ed.): *Arboreal Group Theory*
20 Dazord/Weinstein (eds.): *Symplectic Geometry, Groupoids, and Integrable Systems*
21 Moschovakis (ed.): *Logic from Computer Science*
22 Ratiu (ed.): *The Geometry of Hamiltonian Systems*
23 Baumslag/Miller (eds.): *Algorithms and Classification in Combinatorial Group Theory*
24 Montgomery/Small (eds.): *Noncommutative Rings*
25 Akbulut/King: *Topology of Real Algebraic Sets*
26 Judah/Just/Woodin (eds.): *Set Theory of the Continuum*
27 Carlsson/Cohen/Hsiang/Jones (eds.): *Algebraic Topology and Its Applications*
28 Clemens/Kollár (eds.): *Current Topics in Complex Algebraic Geometry*
29 Nowakowski (ed.): *Games of No Chance*
30 Grove/Petersen (eds.): *Comparison Geometry*
31 Levy (ed.): *Flavors of Geometry*
32 Cecil/Chern (eds.): *Tight and Taut Submanifolds*
33 Axler/McCarthy/Sarason (eds.): *Holomorphic Spaces*
34 Ball/Milman (eds.): *Convex Geometric Analysis*
35 Levy (ed.): *The Eightfold Way*
36 Gavosto/Krantz/McCallum (eds.): *Contemporary Issues in Mathematics Education*
37 Schneider/Siu (eds.): *Several Complex Variables*
38 Billera/Björner/Green/Simion/Stanley (eds.): *New Perspectives in Geometric Combinatorics*
39 Haskell/Pillay/Steinhorn (eds.): *Model Theory, Algebra, and Geometry*
40 Bleher/Its (eds.): *Random Matrix Models and Their Applications*
41 Schneps (ed.): *Galois Groups and Fundamental Groups*
42 Nowakowski (ed.): *More Games of No Chance*
43 Montgomery/Schneider (eds.): *New Directions in Hopf Algebras*
44 Buhler/Stevenhagen (eds.): *Algorithmic Number Theory*
45 Jensen/Ledet/Yui: *Generic Polynomials: Constructive Aspects of the Inverse Galois Problem*
46 Rockmore/Healy (eds.): *Modern Signal Processing*
47 Uhlmann (ed.): *Inside Out: Inverse Problems and Applications*
48 Gross/Kotiuga: *Electromagnetic Theory and Computation: A Topological Approach*
49 Darmon/Zhang (eds.): *Heegner Points and Rankin L-Series*
50 Bao/Bryant/Chern/Shen (eds.): *A Sampler of Riemann–Finsler Geometry*
51 Avramov/Green/Huneke/Smith/Sturmfels (eds.): *Trends in Commutative Algebra*
52 Goodman/Pach/Welzl (eds.): *Combinatorial and Computational Geometry*
53 Schoenfeld (ed.): *Assessing Mathematical Proficiency*
54 Hasselblatt (ed.): *Dynamics, Ergodic Theory, and Geometry*
55 Pinsky/Birnir (eds.): *Probability, Geometry and Integrable Systems*

Volumes 1–4, 6–8 and 10–27 are published by Springer-Verlag

Algorithmic Number Theory:
Lattices, Number Fields, Curves and Cryptography

Edited by

J. P. Buhler
P. Stevenhagen

CAMBRIDGE
UNIVERSITY PRESS

J. P. Buhler
CCR and Reed College
4320 Westerra Ct., San Diego, CA 92121
jpb@reed.edu

P. Stevenhagen
Mathematisch Instituut, Universiteit Leiden
Postbus 9512, 2300 RA Leiden, The Netherlands
psh@math.leidenuniv.nl

Silvio Levy (*Series Editor*)
Mathematical Sciences Research Institute
17 Gauss Way, Berkeley, CA 94720
levy@msri.org

The Mathematical Sciences Research Institute wishes to acknowledge support by the National Science Foundation and the *Pacific Journal of Mathematics* for the publication of this series.

CAMBRIDGE UNIVERSITY PRESS
Cambridge, New York, Melbourne, Madrid, Cape Town, Singapore, São Paulo, Delhi

Cambridge University Press
32 Avenue of the Americas, New York, NY 10013-2473, USA

www.cambridge.org
Information on this title: www.cambridge.org/9780521808545

© Mathematical Sciences Research Institute 2008

This publication is in copyright. Subject to statutory exception
and to the provisions of relevant collective licensing agreements,
no reproduction of any part may take place without
the written permission of Cambridge University Press.

First published 2008

Printed in the United States of America

A catalog record for this publication is available from the British Library.

Library of Congress Cataloging in Publication data

ISBN 978-0-521-80854-5 hardback

Cambridge University Press has no responsibility for the persistence or accuracy of URLs for external or third-party Internet Web sites referred to in this publication and does not guarantee that any content on such Web sites is, or will remain, accurate or appropriate.