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:
Lattices, Number Fields, Curves and Cryptography

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: Lattices, Number Fields, Curves and Cryptography*
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

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

Algorithmic number theory / edited by J. P. Buhler and P. Stevenhagen.
p. cm. – (Mathematical Sciences Research Institute publications ; 44)
Includes bibliographical references and index.
ISBN 978-0-521-80854-5 (hardback)
1. Number theory. 2. Algorithms. 3. Algebraic fields–Data processing. 4. Number theory–Data processing. 5. Factorization (Mathematics) 6. Lattice theory. 7. Curves, Elliptic. 8. Class field theory. I. Buhler, Joe P., 1950– II. Stevenhagen, P., 1963– III. Title. IV. Series.

QA241.S8295 2008
512.7–dc22 2008031327

ISBN 978-0-521-80854-5 hardback

Algorithmic Number Theory
MSRI Publications
Volume **44**, 2008

Contents

Algorithmic Number Theory
MSRI Publications
Volume **44**, 2008

Preface

Our subject arises out of two roots of mathematical thought: fascination with properties of whole numbers and the urge to compute. Number theory and computer science flowered vividly during the last quarter of the twentieth century, and the synergy at their intersection was striking. Algorithmic number theory emerged as an exciting field in its own right, containing deep insights and having surprising applications.

In the fall of 2000 the Mathematical Sciences Research Institute, Berkeley, hosted a one-semester program on algorithmic number theory. Its opening workshop, cosponsored by the Clay Mathematics Institute, featured many foundational and survey talks. During the meeting, it was noted that there was a dearth of sources for newcomers to the field. After the conference, some of the speakers agreed to write articles based on their talks, and we were drafted to edit the volume.

A few authors turned in drafts promptly, some retaining the tutorial focus and tone of the original talks, while others were full-blown tutorials or surveys. Many authors (including the editors) dallied. Additional articles were solicited, to provide more coherence and to incorporate newer results that couldn't be ignored (most notably, the polynomial-time primality algorithm due to Manindra Agrawal, Neeraj Kayal, and Nitin Saxena). This led to complications that might have been expected for a volume with 20 substantial articles, 15 authors, and 650 pages. These have finally run their course, and we are delighted that the volume is ready to see the light of day.

We do apologize to the authors who responded promptly, and can only hope that they will be compensated by the greater breadth and interest of the volume in which their contributions appear.

The articles in the volume can be loosely categorized as follows. The first two articles are introductory, and are more elementary than their successors — they attempt to entice the reader into pursuing the ideas more deeply. The next eight articles provide surveys of central topics, including smooth numbers, factoring, primality testing, lattices, elliptic curves, algebraic number theory, and fast arithmetic algorithms. The remaining ten articles study specific topics more deeply,

including cryptography, computational algebraic number theory, modular forms, and arithmetic geometry.

Although the articles in this volume are surveys in the broadest sense, the word should not be taken to mean an encyclopedic treatment that captures current conventional wisdom. We prefer the term overviews, and the articles have a distinctive and in some cases even nonstandard perspective.

It remains our pleasant duty to thank a number of institutions and people. Most obviously, the authors have produced many fascinating pages, sure to inspire others to pursue the subject. We thank the Clay Institute and MSRI for their generous funding for the workshop that provided the initial spark for this volume. We thank Cambridge University Press and MSRI for their support and patience during the production of this volume, and we especially thank Silvio Levy for his extensive efforts on this volume. John Voight took notes (by typing nearly real-time TEX into his laptop) at most of the talks at the workshop, and these were valuable to some of the authors.

Finally, Hendrik Lenstra has long been a source of pervasive and brilliant inspiration to the entire field of algorithmic number theory, and this volume is no exception: in addition to two distinctive articles, he has provided much-appreciated advice over the years to the editors and to virtually all of the other authors.

Joe Buhler
Peter Stevenhagen
San Diego, May 2008