

Cambridge University Press

978-0-521-80854-5 - Algorithmic Number Theory: Lattices, Number Fields, Curves and
Cryptography

Edited by J. P. Buhler and P. Stevenhagen

Copyright Information

[More information](#)

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

Edited by

J. P. Buhler
P. Stevenhagen



CAMBRIDGE
UNIVERSITY PRESS

Cambridge University Press

978-0-521-80854-5 - Algorithmic Number Theory: Lattices, Number Fields, Curves and
Cryptography

Edited by J. P. Buhler and P. Stevenhagen

Copyright Information

[More information](#)

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.orgInformation 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*

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

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. Information regarding prices, travel timetables, and other factual information given in this work are correct at the time of first printing, but Cambridge University Press does not guarantee the accuracy of such information thereafter.