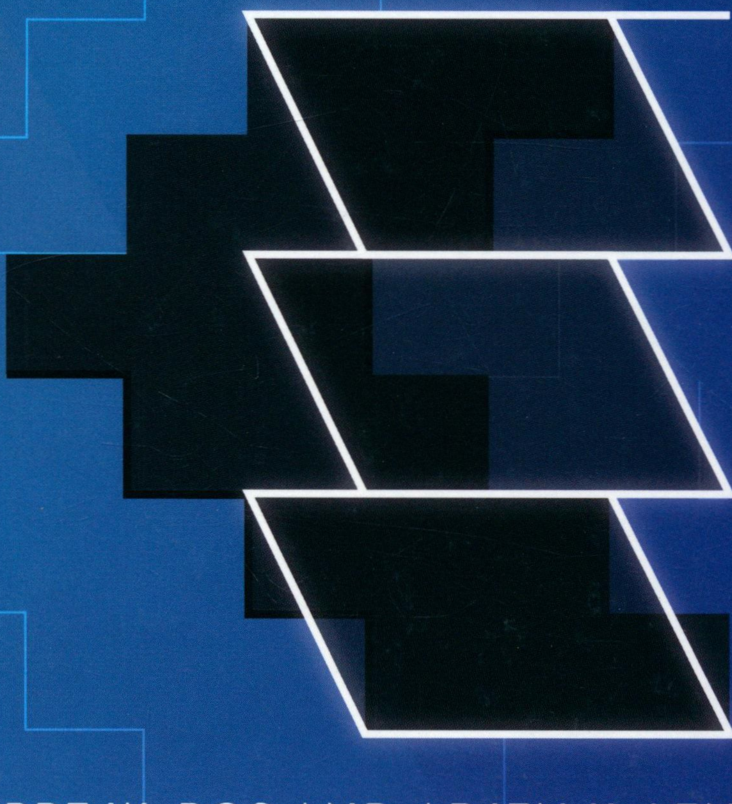
TOPICS IN COMPUTATIONAL NUMBER THEORY

INSPIRED BY PETER L. MONTGOMERY



JOPPE W. BOS AND ARJEN K. LENSTRA

Peter L. Montgomery has made significant contributions to computational number theory, introducing many basic tools such as Montgomery multiplication, Montgomery simultaneous inversion, Montgomery curves, and the Montgomery ladder. This book features state-of-the-art research in computational number theory related to Montgomery's work and its impact on computational efficiency and cryptography. It covers a wide range of topics such as Montgomery multiplication for both hardware and software implementations; Montgomery curves and twisted Edwards curves as proposed in the latest standards for elliptic curve cryptography; and cryptographic pairings. This book provides a comprehensive overview of integer factorization techniques, including dedicated chapters on polynomial selection, the block Lanczos method, and the FFT extension for algebraic-group factorization algorithms. Graduate students and researchers in applied number theory and cryptography will benefit from this survey of Montgomery's work.

Joppe W. Bos is a cryptographic researcher at the Innovation Center for Cryptography & Security at NXP Semiconductors. He also currently serves as the Secretary of the International Association for Cryptologic Research (IACR). His research focuses on computational number theory and high-performance arithmetic as used in public-key cryptography.

Arjen K. Lenstra is Professor of Computer Science at École Polytechnique Fédérale de Lausanne. His research focuses on cryptography and computational number theory, especially in areas such as integer factorization. He was closely involved in the development of the number field sieve method for integer factorization as well as several other cryptologic results. He is the recipient of the Excellence in the Field of Mathematics RSA Conference 2008 Award and a Fellow of the International Association for Cryptologic Research (IACR).

CAMBRIDGE
UNIVERSITY PRESS
www.cambridge.org

ISBN 978-1-107-10935-3

9 781107 109353

TOPICS IN
COMPUTATIONAL
NUMBER THEORY

INSPIRED BY
PETER L.
MONTGOMERY

JOPPE W.
BOS
AND
ARJEN K.
LENSTRA

CAMBRIDGE

Topics in Computational Number Theory Inspired by Peter L. Montgomery

Edited by

JOPPE W. BOS
NXP Semiconductors, Leuven, Belgium

ARJEN K. LENSTRA
EPFL, Lausanne, Switzerland

CAMBRIDGE
UNIVERSITY PRESS

CAMBRIDGE
UNIVERSITY PRESS

University Printing House, Cambridge CB2 8BS, United Kingdom

One Liberty Plaza, 20th Floor, New York, NY 10006, USA

477 Williamstown Road, Port Melbourne, VIC 3207, Australia

4843/24, 2nd Floor, Ansari Road, Daryaganj, Delhi - 110002, India

79 Anson Road, #06-04/06, Singapore 079906

Cambridge University Press is part of the University of Cambridge.

It furthers the University's mission by disseminating knowledge in the pursuit of education, learning, and research at the highest international levels of excellence.

www.cambridge.org
Information on this title: www.cambridge.org/9781107109353
DOI: 10.1017/9781316271575

First published 2017

Printed in the United Kingdom by Clays, St Ives plc

A catalogue record for this publication is available from the British Library

Library of Congress Cataloging-in-Publication data
Names: Bos, Joppe W., editor. | Lenstra, A. K. (Arjen K.), 1956– editor.
Title: Topics in computational number theory inspired by Peter L. Montgomery / edited by Joppe W. Bos, NXP Semiconductors, Belgium; Arjen K. Lenstra, EPFL, Lausanne, Switzerland.
Description: Cambridge : Cambridge University Press, 2017. | Series: London Mathematical Society lecture note series | Includes bibliographical references and index.
Identifiers: LCCN 2017023049 | ISBN 9781107109353 (pbk. : alk. paper)
Subjects: LCSH: Number theory. | Cryptography – Mathematics. | Montgomery, Peter L., 1947–
Classification: LCC QA241 .T657 2017 | DDC 512.7 – dc23 LC record available at https://lccn.loc.gov/2017023049

ISBN 978-1-107-10935-3 Paperback

Topics in Computational Number Theory Inspired by Peter L. Montgomery

Peter L. Montgomery has made significant contributions to computational number theory, introducing many basic tools such as Montgomery multiplication, Montgomery simultaneous inversion, Montgomery curves, and the Montgomery ladder. This book features state-of-the-art research in computational number theory related to Montgomery's work and its impact on computational efficiency and cryptography. It covers a wide range of topics such as Montgomery multiplication for both hardware and software implementations; Montgomery curves and twisted Edwards curves as proposed in the latest standards for elliptic curve cryptography; and cryptographic pairings. This book provides a comprehensive overview of integer factorization techniques, including dedicated chapters on polynomial selection, the block Lanczos method, and the FFT extension for algebraic-group factorization algorithms. Graduate students and researchers in applied number theory and cryptography will benefit from this survey of Montgomery's work.

Joppe W. Bos is a cryptographic researcher at the Innovation Center for Cryptography & Security at NXP Semiconductors. He also currently serves as the Secretary of the International Association for Cryptologic Research (IACR). His research focuses on computational number theory and high-performance arithmetic as used in public-key cryptography.

Arjen K. Lenstra is Professor of Computer Science at École Polytechnique Fédérale de Lausanne. His research focuses on cryptography and computational number theory, especially in areas such as integer factorization. He was closely involved in the development of the number field sieve method for integer factorization as well as several other cryptologic results. He is the recipient of the Excellence in the Field of Mathematics RSA Conference 2008 Award and a Fellow of the International Association for Cryptologic Research (IACR).

Contributors

Joppe W. Bos, *NXP Semiconductors, Leuven, Belgium*

Arjen K. Lenstra, *EPFL, Lausanne, Switzerland*

Herman te Riele, *CWI, Amsterdam, Netherlands*

Daniel Shumow, *Microsoft Research, Redmond, USA*

Peter L. Montgomery, *Self*

Colin D. Walter, *Royal Holloway, University of London, Egham, United Kingdom*

Daniel J. Bernstein, *University of Illinois at Chicago, Chicago, USA and Technische Universiteit Eindhoven, Eindhoven, The Netherlands*

Tanja Lange, *Technische Universiteit Eindhoven, Eindhoven, The Netherlands*

Thorsten Kleinjung, *University Leipzig, Leipzig, Germany and EPFL, Lausanne, Switzerland*

Emmanuel Thomé, *Inria, Nancy, France*

Richard P. Brent, *Australian National University, Canberra, Australia*

Alexander Kruppa, *Technische Universität München, München, Germany*

Paul Zimmermann, *Inria/LORIA, Nancy, France*

Kristin Lauter, *Microsoft Research, Redmond, USA*

Michael Naehrig, *Microsoft Research, Redmond, USA*

Preface

This book was written in honor of Peter L. Montgomery and his inspirational contributions to computational number theory. The editors would like to extend their sincerest thanks to all authors for their enthusiastic response to our invitation to contribute, and to Nicole Verna for the cover design.

Contents