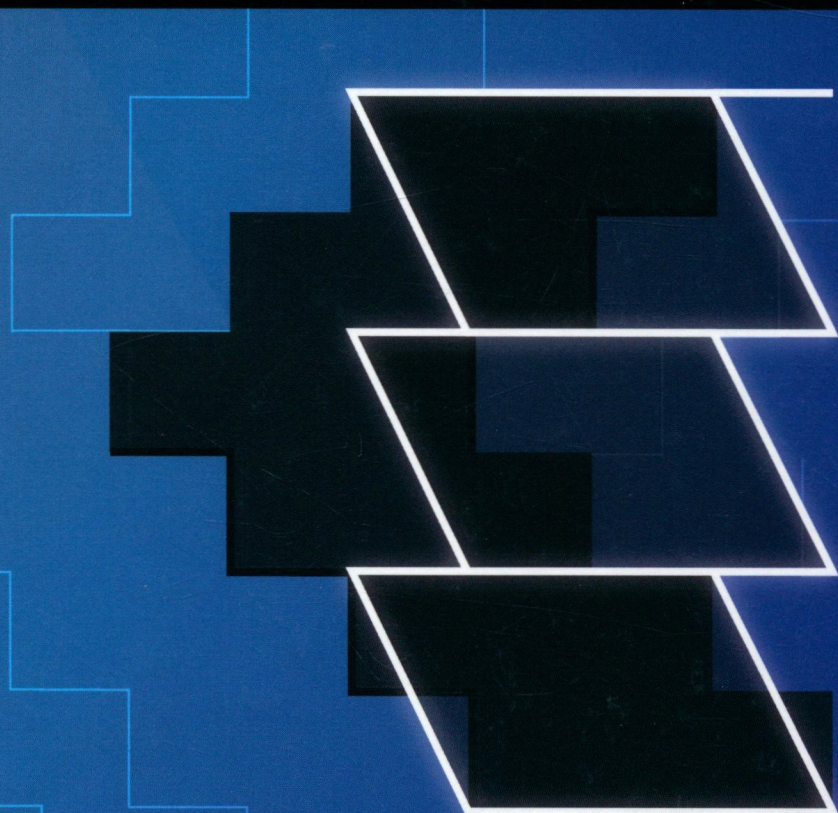


TOPICS IN _____

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



TOPICS IN
COMPUTATIONAL
NUMBER THEORY

INSPIRED BY
PETER L.
MONTGOMERY

JOPPE W.
BOŠ
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

© Joppe W. Bos and Arjen K. Lenstra 2017

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 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://lcn.loc.gov/2017023049>

ISBN 978-1-107-10935-3 Paperback

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.

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

<i>List of Contributors</i>	page xi
<i>Preface</i>	xiii
1 Introduction	1
1.1 Outline	1
1.2 Biographical Sketch	1
1.3 Overview	5
1.4 Simultaneous Inversion	8
2 Montgomery Arithmetic from a Software Perspective	10
2.1 Introduction	10
2.2 Montgomery Multiplication	12
2.2.1 Interleaved Montgomery Multiplication	15
2.2.2 Using Montgomery Arithmetic in Practice	16
2.2.3 Computing the Montgomery Constants μ and R^2	18
2.2.4 On the Final Conditional Subtraction	19
2.2.5 Montgomery Multiplication in \mathbb{F}_{2^t}	21
2.3 Using Primes of a Special Form	22
2.3.1 Faster Modular Reduction with Primes of a Special Form	23
2.3.2 Faster Montgomery Reduction with Primes of a Special Form	24
2.4 Concurrent Computing of Montgomery Multiplication	26
2.4.1 Related Work on Concurrent Computing of Montgomery Multiplication	27
2.4.2 Montgomery Multiplication Using SIMD Extensions	27
2.4.3 A Column-Wise SIMD Approach	31

2.4.4	Montgomery Multiplication Using the Residue Number System Representation	36
3	Hardware Aspects of Montgomery Modular Multiplication	40
3.1	Introduction and Summary	40
3.2	Historical Remarks	42
3.3	Montgomery's Novel Modular Multiplication Algorithm	42
3.4	Standard Acceleration Techniques	43
3.5	Shifting the Modulus N	44
3.5.1	The Classical Algorithm	44
3.5.2	Montgomery	45
3.6	Interleaving Multiplication Steps with Modular Reduction	46
3.7	Accepting Inaccuracy in Quotient Digits	48
3.7.1	Traditional	48
3.7.2	Bounding the Partial Product	50
3.7.3	Montgomery	52
3.7.4	Summary	52
3.8	Using Redundant Representations	53
3.8.1	Traditional	54
3.8.2	Montgomery	54
3.9	Changing the Size of the Hardware Multiplier	55
3.10	Shifting an Operand	57
3.10.1	Traditional	57
3.10.2	Montgomery	60
3.11	Precomputing Multiples of B and N	61
3.12	Propagating Carries and Carry-Save Inputs	62
3.13	Scaling the Modulus	65
3.14	Systolic Arrays	67
3.14.1	A Systolic Array for $A \times B$	68
3.14.2	Scalability	70
3.14.3	A Linear Systolic Array	72
3.14.4	A Systolic Array for Modular Multiplication	73
3.15	Side-Channel Concerns and Solutions	76
3.16	Logic Gate Technology	80
3.17	Conclusion	81
4	Montgomery Curves and the Montgomery Ladder	82
4.1	Introduction	82
4.2	Fast Scalar Multiplication on the Clock	83

4.2.1	The Lucas Ladder	85
4.2.2	Differential Addition Chains	85
4.3	Montgomery Curves	87
4.3.1	Montgomery Curves as Weierstrass Curves	87
4.3.2	The Group Law for Weierstrass Curves	88
4.3.3	Other Views of the Group Law	89
4.3.4	Edwards Curves and Their Group Law	90
4.3.5	Montgomery Curves as Edwards Curves	92
4.3.6	Elliptic-Curve Cryptography (ECC)	93
4.3.7	Examples of Noteworthy Montgomery Curves	94
4.4	Doubling Formulas without y	95
4.4.1	Doubling: The Weierstrass View	95
4.4.2	Optimized Doublings	96
4.4.3	A Word of Warning: Projective Coordinates	97
4.4.4	Completeness of Generic Doubling Formulas	97
4.4.5	Doubling: The Edwards View	98
4.5	Differential-Addition Formulas	99
4.5.1	Differential Addition: The Weierstrass View	99
4.5.2	Optimized Differential Addition	101
4.5.3	Quasi-Completeness	101
4.5.4	Differential Addition: The Edwards View	103
4.6	The Montgomery Ladder	104
4.6.1	The Montgomery Ladder Step	104
4.6.2	Constant-Time Ladders	105
4.6.3	Completeness of the Ladder	106
4.7	A Two-Dimensional Ladder	107
4.7.1	Introduction to the Two-Dimensional Ladder	108
4.7.2	Recursive Definition of the Two-Dimensional Ladder	109
4.7.3	The Odd-Odd Pair in Each Line: First Addition	110
4.7.4	The Even-Even Pair in Each Line: Doubling	110
4.7.5	The Other Pair in Each Line: Second Addition	111
4.8	Larger Differences	111
4.8.1	Examples of Large-Difference Chains	112
4.8.2	CFRC, PRAC, etc.	114
4.8.3	Allowing d to Vary	114
5	General Purpose Integer Factoring	116
5.1	Introduction	116
5.2	General Purpose Factoring	117

5.2.1	Two-Step Approach	117
5.2.2	Smoothness and L -notation	119
5.2.3	Generic Analysis	120
5.2.4	Smoothness Testing	121
5.2.5	Finding Dependencies	123
5.2.6	Filtering	123
5.2.7	Overall Effort	126
5.3	Presieving General Purpose Factoring	126
5.3.1	Dixon's Random Squares Method	126
5.3.2	Continued Fraction Method	127
5.4	Linear and Quadratic Sieve	129
5.4.1	Linear Sieve	129
5.4.2	Quadratic Sieving: Plain	132
5.4.3	Quadratic Sieving: Fancy	133
5.4.4	Multiple Polynomial Quadratic Sieve	134
5.5	Number Field Sieve	137
5.5.1	Earlier Methods to Compute Discrete Logarithms	139
5.5.2	Special Number Field Sieve	145
5.5.3	General Number Field Sieve	152
5.5.4	Coppersmith's Modifications	158
5.6	Provable Methods	160
6	Polynomial Selection for the Number Field Sieve	161
6.1	The Problem	161
6.2	Early Methods	161
6.3	General Remarks	164
6.4	A Lattice Based Method	166
6.5	Skewness	168
6.6	Base m Method and Skewness	170
6.7	Root Sieve	171
6.8	Later Developments	173
7	The Block Lanczos Algorithm	175
7.1	Linear Systems for Integer Factoring	175
7.2	The Standard Lanczos Algorithm	176
7.3	The Case of Characteristic Two	179
7.4	Orthogonalizing a Sequence of Subspaces	180
7.5	Construction of the Next Iterate	181
7.6	Simplifying the Recurrence Equation	182
7.7	Termination	184
7.8	Implementation in Parallel	186
7.9	Recent Developments	187

8	FFT Extension for Algebraic-Group Factorization Algorithms	189
8.1	Introduction	189
8.2	FFT Extension for the Elliptic Curve Method	191
8.2.1	The Product Tree Algorithm	192
8.2.2	The POLYEVAL Algorithm	192
8.2.3	The POLYGCD Algorithm	195
8.2.4	Choice of Points of Evaluation	197
8.2.5	A Numerical Example	199
8.3	FFT Extension for the $p - 1$ and $p + 1$ Methods	199
8.3.1	Constructing $F(X)$ by Scaling and Multiplying	201
8.3.2	Evaluation of a Polynomial Along a Geometric Progression	202
9	Cryptographic Pairings	206
9.1	Preliminaries	207
9.1.1	Elliptic Curves	208
9.1.2	Pairings	209
9.1.3	Pairing-Friendly Elliptic Curves	213
9.2	Finite Field Arithmetic for Pairings	213
9.2.1	Montgomery Multiplication	214
9.2.2	Multiplication in Extension Fields	215
9.2.3	Finite Field Inversions	215
9.2.4	Simultaneous Inversions	218
9.3	Affine Coordinates for Pairing Computation	219
9.3.1	Costs for Doubling and Addition Steps	219
9.3.2	Working over Extension Fields	223
9.3.3	Simultaneous Inversions in Pairing Computation	225
9.4	The Double-Add Operation and Parabolas	227
9.4.1	Description of the Algorithm	228
9.4.2	Application to Scalar Multiplication	229
9.4.3	Application to Pairings	229
9.5	Squared Pairings	231
9.5.1	The Squared Weil Pairing	232
9.5.2	The Squared Tate Pairing	233
	<i>Bibliography</i>	235
	<i>Subject Index</i>	261

