Lecture Notes in Mathematics 1554

Editors:
A. Dold, Heidelberg
B. Eckmann, Zürich
F. Takens, Groningen

A. K. Lenstra H. W. Lenstra, Jr. (Eds.)

The development of the number field sieve

Springer-Verlag
Berlin Heidelberg New York
London Paris Tokyo
Hong Kong Barcelona
Budapest

Editors

Arjen K. Lenstra
Room MRE-2Q334
Bellcore
445 South Street
Morristown, NJ 07960, USA
E-mail: lenstra@bellcore.com

Hendrik W. Lenstra, Jr.
Department of Mathematics
University of California
Berkeley, CA 94720, USA
E-mail: hwl@math.berkeley.edu

Mathematics Subject Classification (1991): 11Y05, 11Y40

ISBN 3-540-57013-6 Springer-Verlag Berlin Heidelberg New York
ISBN 0-387-57013-6 Springer-Verlag New York Berlin Heidelberg

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer-Verlag. Violations are liable for prosecution under the German Copyright Law.

© Springer-Verlag Berlin Heidelberg 1993
Printed in Germany

46/3140-543210 - Printed on acid-free paper

PREFACE

The number field sieve is an algorithm for factoring integers that John Pollard proposed in 1988. This volume contains six papers on the number field sieve. They are preceded by an annotated bibliography, to which we refer for a brief description of the contents of each individual paper.

We assume the reader to be familiar with the basic techniques that underlie modern integer factoring methods. An introduction to these techniques is given in:

> A. K. Lenstra, H. W. Lenstra, Jr., M. S. Manasse, J. M. Pollard, *The factorization of the ninth Fermat number*, Math. Comp. **61** (1993), to appear.

The same paper includes a discussion of tools from algebraic number theory that the number field sieve depends on. Comprehensive accounts of older algorithms for factoring integers and related problems, with extensive bibliographies, can be found in:

> A. K. Lenstra, H. W. Lenstra, Jr., *Algorithms in number theory*, Chapter 12 in: J. van Leeuwen (ed.), *Handbook of theoretical computer science*, Volume A, *Algorithms and complexity*, Elsevier, Amsterdam, 1990,

> C. Pomerance (ed.), *Cryptology and computational number theory*, Proc. Sympos. Appl. Math. **42**, Amer. Math. Soc., Providence, 1990.

The developments leading up to the number field sieve are sketched on pp. 11–13 below. The annotated bibliography (pp. 1–3) tells, implicitly, the recent history of the number field sieve itself.

We express our gratitude to the authors of the papers for contributing their work to this volume. In particular we wish to thank Carl Pomerance for conceiving the idea of a combined publication and for advising us in all stages of its execution. In addition, we thank Henri Cohen, Dan Gordon, Andrew Odlyzko, Jonathan Pila, and Tom Trotter for their assistance.

We gratefully acknowledge the use of the $\mathcal{A}\mathcal{M}\mathcal{S}$-TeX typesetting package.

The editors

CONTENTS

The number field sieve: an annotated bibliography 1
H. W. Lenstra, Jr.

Factoring with cubic integers 4
J. M. Pollard

Introduction 4
Properties of the set S 5
Operations on the integers of S 6
Factorisation of F_7 7
Computer and program details 9
Example of an A-solution 10
References 10

The number field sieve 11
A. K. Lenstra, H. W. Lenstra, Jr., M. S. Manasse, J. M. Pollard

1. Introduction 11
2. The algorithm 14
3. Finding generators 20
4. Sieving 25
5. Finding the unit contribution 29
6. Run time analysis 30
7. Additional remarks 33
8. Examples 34
9. Generalization 38

References 40

The lattice sieve 43
J. M. Pollard

Object of the lattice sieve 43
Operation of the sieve 45
More factorisations of F_7! 46
Some programming notes 48
Numerical example from the factorisation of F_7 49
References 49

Factoring integers with the number field sieve 50
J. P. Buhler, H. W. Lenstra, Jr., Carl Pomerance

1. Introduction 50
2. The idea of the number field sieve 52
3. Finding a polynomial 54
4. The rational sieve 55
5. The algebraic sieve 57
6. Four obstructions 60

7. Algebraic interlude 63
8. Quadratic characters 67
9. Finding square roots 70
10. Analytic interlude 76
11. Summary of the number field sieve and a heuristic analysis 80
12. Homogeneous polynomials 84
References 92

Computing a square root for the number field sieve **95**
Jean-Marc Couveignes

1. Introduction 95
2. Description and analysis of the method 98
References 102

A general number field sieve implementation **103**
Daniel J. Bernstein, A. K. Lenstra

1. Introduction 103
2. Outline of the implementation 104
3. Choosing the polynomial 104
4. Searching for a polynomial 107
5. Computing bases 108
6. Sieving 108
7. Trial dividing 114
8. Constructing the matrix 115
9. Reducing the matrix 116
10. Computing the square root 116
11. Proof that the square root works 118
12. Examples 120
13. Future directions 124
References 125

The illustration on the front cover **127**

Index **129**