

Henri Cohen (Ed.)

# Algorithmic Number Theory

Second International Symposium, ANTS-II  
Talence, France, May 18-23, 1996  
Proceedings



Springer

Series Editors

Gerhard Goos, Karlsruhe University, Germany

Juris Hartmanis, Cornell University, NY, USA

Jan van Leeuwen, Utrecht University, The Netherlands

Volume Editor

Henri Cohen

Laboratoire A2X, Université Bordeaux I

351 Cours de la Libération, F-33505 Talence Cedex, France

Cataloging-in-Publication data applied for

### Die Deutsche Bibliothek - CIP-Einheitsaufnahme

**Algorithmic number theory : second international symposium ; proceedings / ANTS 2, Talence, France, May 18 - 23, 1996 / Henri Cohen (ed.). - Berlin ; Heidelberg ; New York ; Barcelona ; Budapest ; Hong Kong ; London ; Milan ; Paris ; Santa Clara ; Singapore ; Tokyo : Springer, 1996**  
(Lecture notes in computer science ; Vol. 1122)

ISBN 3-540-61581-4

NE: Cohen, Henri [Hrsg.]; ANTS <2, 1996, Talence>; GT

CR Subject Classification (1991): I.1, F.2.2, G.2, E.3-4, J.2

1991 Mathematics Subject Classification: 11Yxx, 11T71, 68P25, 68Q40, 68Q25, 68Q20, 12Y05, 94A60

ISSN 0302-9743

ISBN 3-540-61581-4 Springer-Verlag Berlin Heidelberg New York

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 1996  
Printed in Germany

Typesetting: Camera-ready by author

SPIN 10513479 06/3142 - 5 4 3 2 1 0 Printed on acid-free paper

# Table of Contents

Adleman, L. M. and Huang, M.-D. <i>Counting Rational Points on Curves and Abelian Varieties over Finite Fields</i> .....	1
Belabas, K. <i>Computing Cubic Fields in Quasi-Linear Time</i> .....	17
Bernstein, D. J. <i>Fast Ideal Arithmetic via Lazy Localization</i> .....	27
Brent, R. P., van der Poorten, A. J. and te Riele, H. J. <i>A Comparative Study of Algorithms for Computing Continued Fractions of Algebraic Numbers</i> .....	35
Cohen, H., Diaz y Diaz, F. and Olivier, M. <i>Computing Ray Class Groups, Conductors and Discriminants</i> .....	49
Couveignes, J.-M. <i>Computing <math>l</math>-Isogenies Using the <math>p</math>-Torsion</i> .....	59
Daberkow, M. and Pohst, M. E. <i>On Computing Hilbert Class Fields of Prime Degree</i> .....	67
Denny, T. F. and Müller, V. <i>On the Reduction of Composed Relations from the Number Field Sieve</i> .....	75
Dummit, D. S. and Hayes, D. R. <i>Checking the <math>p</math>-adic Stark Conjecture When <math>p</math> Is Archimedean</i> .....	91
Elkenbracht-Huizing, M. <i>A Multiple Polynomial General Number Field Sieve</i> .....	99
Fermigier, S. <i>Construction of High-Rank Elliptic Curves over <math>\mathbb{Q}</math> and <math>\mathbb{Q}(t)</math> with Non-Trivial 2-Torsion</i> .....	115
ní Fhlathúin, B. <i>The Height on an Abelian Variety</i> .....	121

Fieker, C. and Pohst, M. E. <i>On Lattices over Number Fields</i> .....	133
Ford, D. <i>Minimum Discriminants of Primitive Sextic Fields</i> .....	141
Ford, D. and Havas, G. <i>A New Algorithm and Refined Bounds for Extended Gcd Computation</i> ..	145
Gaál, I. <i>Application of Thue Equations to Computing Power Integral Bases in Algebraic Number Fields</i> .....	151
Gebel, J., Pethő, A. and Zimmer, H. G. <i>Computing <math>S</math>-Integral Points on Elliptic Curves</i> .....	157
Giesbrecht, M. <i>Probabilistic Computation of the Smith Normal Form of a Sparse Integer Matrix</i> .....	173
Lauter, K. <i>Ray Class Field Constructions of Curves over Finite Fields with Many Rational Points</i> .....	187
Lercier, R. <i>Computing Isogenies in <math>\mathbb{F}_{2^n}</math></i> .....	197
Louboutin, S. <i>A Computational Technique for Determining Relative Class Numbers of CM-Fields</i> .....	213
McKee, J. and Pinch, R. <i>Old and New Deterministic Factoring Algorithms</i> .....	217
Meyer, S. M. and Sorenson, J. P. <i>Efficient Algorithms for Computing the Jacobi Symbol</i> .....	225
Niklasch, G. <i>The Number Field Database on the World Wide Web Server</i> .....	241
Paulus, S. <i>An Algorithm of Subexponential Type Computing the Class Group of Quadratic Orders over Principal Ideal Domains</i> .....	243
Pohst, M. E. (Invited talk) <i>Computational Aspects of Kummer Theory</i> .....	259

Pohst, M. E. and Schörning, M. <i>On Integral Basis Reduction in Global Function Fields</i> .....	273
Poonen, B. (Invited talk) <i>Computational Aspects of Curves of Genus at Least 2</i> .....	283
Rössner, C. and Seifert, J.-P. <i>The Complexity of Approximate Optima for Greatest Common Divisor Computations</i> .....	307
Scheidler, R. <i>Compact Representation in Real Quadratic Congruence Function Fields</i> .....	323
Schirokauer, O., Weber, D. and Denny, T. (Invited talk) <i>Discrete Logarithms: The Effectiveness of the Index Calculus Method</i> .....	337
Smart, N. <i>How Difficult Is It to Solve a Thue Equation?</i> .....	363
Stein, A. <i>Elliptic Congruence Function Fields</i> .....	375
Tsfasman, M. (Invited talk) <i>Algebraic Geometry Lattices and Codes</i> .....	385
Weber, D. <i>Computing Discrete Logarithms with the General Number Field Sieve</i> .....	391
<b>Author Index</b> .....	405