Lecture Notes in Computer Science 1122
Edited by G. Goos, J. Hartmanis and J. van Leeuwen

Advisory Board: W. Brauer D. Gries J. Stoer

Henri Cohen (Ed.)

Algorithmic Number Theory

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

Springer

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

Typesetting: Camera-ready by author
SPIN 10513479 06/3142 – 5 4 3 2 1 0 Printed on acid-free paper

Preface

The second Algorithmic Number Theory Symposium (ANTS II) was held at the Université Bordeaux I, Talence, France on May 18–23, 1996. There were almost 120 participants, primarily from Europe and North America. It followed the ANTS I conference held at Cornell University in 1994, and it will be followed by ANTS III in 1998, organized by Joe Buhler at Reed College, Portland, Oregon, U.S.A.

The ANTS II conference was sponsored by the French Délégation Générale à l'Armement (DGA)[1], by the Ministry of Education and Research (MESR), by the Centre National de la Recherche Scientifique (CNRS), by the Région Aquitaine, by the Université Bordeaux I, by the Laboratoire A2X, and by Sun Microsystems France. We would like to heartily thank all these organizations and corporations for their support.

The ANTS II conference was organized by Professors Henri Cohen and Michel Olivier, with the help of the staff and students of the Laboratoire A2X. We would like to thank in particular Karim Belabas for his help in the preparation of this volume, Francine Delmer for preparing the posters and the cover of the preproceedings volume given to the participants, Daniel Ynbourg and Mauricette Jaubert for the considerable printing task of the preproceedings, Christian Labesse for installing the computers for the participants, and finally Véronique Saint-Martin for the secretarial work.

The programming committee was headed by Henri Cohen, and consisted of: Johannes Buchmann, Ming-Deh Huang, Jacques Martinet, Francois Morain, Andrew Odlyzko, and René Schoof. We thank them for their time and effort which helped assure the high quality of the symposium.

Le deuxième Symposium de Théorie Algorithmique des Nombres (ANTS II) a eu lieu à l'Université Bordeaux I, Talence, France, du 18 au 23 mai 1996. Ce colloque a réuni près de 120 participants, venant principalement d'Europe et d'Amérique du nord. Il a fait suite au symposium ANTS I qui a eu lieu à l'Université Cornell aux USA en 1994, et sera suivi par ANTS III en 1998, organisé par Joe Buhler à Reed College, Portland, Oregon, U.S.A.

[1] **Contrat 96-1029/A000**

Le colloque ANTS II a été soutenu financièrement par la Délégation Générale à l'Armement (DGA)[2], par le Minisère de l'Éducation et de la Recherche (MESR), par le Centre National de la Recherche Scientifique (CNRS), par la Région Aquitaine, par l'Université Bordeaux I, par le Laboratoire A2X, et par la compagnie Sun France. Nous exprimons notre profonde gratitude à toutes ces organisations et compagnies.

Le colloque ANTS II a été organisé par Henri Cohen et Michel Olivier, avec l'aide du personnel et des étudiants du Laboratoire A2X. Nous remercions tout particulièrement Karim Belabas pour l'aide apportée à la préparation de ce volume, Francine Delmer pour la fabrication de l'affiche du congrès et de la couverture du volume distribué aux participants, Daniel Ynbourg et Mauricette Jaubert pour le gros travail d'impression du volume en question, Christian Labesse pour l'installation des machines mises à la disposition des participants, et enfin Véronique Saint-Martin pour le travail de secrétariat.

Le comité scientifique était dirigé par Henri Cohen, et comprenait: Johannes Buchmann, Ming-Deh Huang, Jacques Martinet, Francois Morain, Andrew Odlyzko et René Schoof. Nous les remercions pour leur temps et leurs efforts qui ont permis d'assurer la plus grande qualité possible à ce colloque.

Henri Cohen

June 27, 1996

[2] **Contrat 96-1029/A000**

Table of Contents

Adleman, L. M. and Huang, M.-D.
Counting Rational Points on Curves and Abelian Varieties over Finite Fields 1

Belabas, K.
Computing Cubic Fields in Quasi-Linear Time 17

Bernstein, D. J.
Fast Ideal Arithmetic via Lazy Localization 27

Brent, R. P., van der Poorten, A. J. and te Riele, H. J.
A Comparative Study of Algorithms for Computing Continued Fractions of Algebraic Numbers 35

Cohen, H., Diaz y Diaz, F. and Olivier, M.
Computing Ray Class Groups, Conductors and Discriminants 49

Couveignes, J.-M.
Computing l-Isogenies Using the p-Torsion 59

Daberkow, M. and Pohst, M. E.
On Computing Hilbert Class Fields of Prime Degree 67

Denny, T. F. and Müller, V.
On the Reduction of Composed Relations from the Number Field Sieve 75

Dummit, D. S. and Hayes, D. R.
Checking the $\mathfrak{p}$-adic Stark Conjecture When $\mathfrak{p}$ Is Archimedean 91

Elkenbracht-Huizing, M.
A Multiple Polynomial General Number Field Sieve 99

Fermigier, S.
Construction of High-Rank Elliptic Curves over $\mathbb{Q}$ and $\mathbb{Q}(t)$ with Non-Trivial 2-Torsion 115

ní Fhlathúin, B.
The Height on an Abelian Variety 121

Fieker, C. and Pohst, M. E.
On Lattices over Number Fields 133

Ford, D.
Minimum Discriminants of Primitive Sextic Fields 141

Ford, D. and Havas, G.
A New Algorithm and Refined Bounds for Extended Gcd Computation .. 145

Gaál, I.
Application of Thue Equations to Computing Power Integral Bases in Algebraic Number Fields 151

Gebel, J., Pethö, A. and Zimmer, H. G.
Computing S-Integral Points on Elliptic Curves 157

Giesbrecht, M.
Probabilistic Computation of the Smith Normal Form of a Sparse Integer Matrix 173

Lauter, K.
Ray Class Field Constructions of Curves over Finite Fields with Many Rational Points 187

Lercier, R.
Computing Isogenies in $\mathbb{F}_{2^n}$ 197

Louboutin, S.
A Computational Technique for Determining Relative Class Numbers of CM-Fields 213

McKee, J. and Pinch, R.
Old and New Deterministic Factoring Algorithms 217

Meyer, S. M. and Sorenson, J. P.
Efficient Algorithms for Computing the Jacobi Symbol 225

Niklasch, G.
The Number Field Database on the World Wide Web Server 241

Paulus, S.
An Algorithm of Subexponential Type Computing the Class Group of Quadratic Orders over Principal Ideal Domains 243

Pohst, M. E. (Invited talk)
Computational Aspects of Kummer Theory 259

Pohst, M. E. and Schörnig, M.
On Integral Basis Reduction in Global Function Fields 273

Poonen, B. (Invited talk)
Computational Aspects of Curves of Genus at Least 2 283

Rössner, C. and Seifert, J.-P.
The Complexity of Approximate Optima for Greatest Common Divisor Computations 307

Scheidler, R.
Compact Representation in Real Quadratic Congruence Function Fields 323

Schirokauer, O., Weber, D. and Denny, T. (Invited talk)
Discrete Logarithms: The Effectiveness of the Index Calculus Method 337

Smart, N.
How Difficult Is It to Solve a Thue Equation? 363

Stein, A.
Elliptic Congruence Function Fields 375

Tsfasman, M. (Invited talk)
Algebraic Geometry Lattices and Codes 385

Weber, D.
Computing Discrete Logarithms with the General Number Field Sieve 391

Author Index 405