

Lecture Notes in Computer Science

1838

Edited by G. Goos, J. Hartmanis, and J. van Leeuwen

Berlin
Heidelberg
New York
Barcelona
Hong Kong
London
Milan
Paris
Singapore
Tokyo

Wieb Bosma (Ed.)

Algorithmic Number Theory

4th International Symposium, ANTS-IV
Leiden, The Netherlands, July 2-7, 2000
Proceedings

Series Editors

Gerhard Goos, Karlsruhe University, Germany
Juris Hartmanis, Cornell University, NY, USA
Jan van Leeuwen, Utrecht University, The Netherlands

Volume Editor

Wieb Bosma
University of Nijmegen, Mathematical Institute
Postbus 9010, 6500 GL Nijmegen, The Netherlands
E-mail: bosma@sci.kun.nl

Cataloging-in-Publication Data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Algorithmic number theory : 4th international symposium ; proceedings /
ANTS-IV, Leiden, The Netherlands, July 2 - 7, 2000. Wieb Bosma
(ed.). - Berlin ; Heidelberg ; New York ; Barcelona ; Hong Kong ;
London ; Milan ; Paris ; Singapore ; Tokyo : Springer, 2000
(Lecture notes in computer science ; Vol. 1838)
ISBN 3-540-67695-3

CR Subject Classification (1998): I.1, F.2.2, G.2, E.3-4, J.2

ISSN 0302-9743

ISBN 3-540-67695-3 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 is a company in the BertelsmannSpringer publishing group.
© Springer-Verlag Berlin Heidelberg 2000
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Christian Grosche, Hamburg
Printed on acid-free paper SPIN: 10722028 06/3142 5 4 3 2 1 0

Preface

The fourth Algorithmic Number Theory Symposium takes place at the Universiteit Leiden, in the Netherlands, from July 2-7, 2000. Its organization is a joint effort of Dutch number theorists from Leiden, Groningen, Nijmegen, and Amsterdam.

Six invited talks and 36 contributed talks are scheduled. This volume contains the written versions of the talks, with the exception of two of the invited talks. Not included are: *A rational approach to π* by Frits Beukers (Utrecht) and *The 40 trillionth binary digit of π is 0* by Peter Borwein (Burnaby, Canada). These talks are aimed at a wider audience, and form part of the special ANTS IV event *Pi in de Pieterskerk* on July 5, 2000. This event includes an evening ceremony in which the tombstone of Ludolph van Ceulen is replaced. Van Ceulen, who was appointed to Leiden in 1600, calculated 35 decimals of π . His tombstone in the Pieterskerk, in which these decimals were engraved, disappeared in the 19th century.

ANTS in Leiden is the fourth in a series of symposia that started in 1994. Previous locations were Cornell University, Ithaca, New York (1994), Université de Bordeaux I in Bordeaux, France (1996), and Reed College, Portland, Oregon (1998). The diversity of the papers contained in this volume shows that the main theme of ANTS, algorithmic number theory, is taken in a broad sense. The number of submissions for the Leiden conference largely exceeded the physical limitations of our one-week schedule. We are therefore confident that we are only at the beginning of a continuing tradition.

May 2000

Peter Stevenhagen
ANTS IV Program Chair
Wieb Bosma
Proceedings Editor

Organization

Organizing Committee

Wieb Bosma (Katholieke Universiteit Nijmegen)
Herman te Riele (CWI, Amsterdam)
Bart de Smit (Universiteit Leiden)
Peter Stevenhagen (Universiteit Leiden)
Jaap Top (Rijksuniversiteit Groningen)

Advisory Board

Dan Boneh (Stanford University)
Joe P. Buhler (Reed College, Portland)
Arjen K. Lenstra (Citibank)
Hendrik W. Lenstra, Jr. (UC Berkeley, and Universiteit Leiden)
Andrew M. Odlyzko (AT&T)
Rob Tijdeman (Universiteit Leiden)

Sponsoring Institutions

The organizers of ANTS IV gratefully acknowledge financial support from the following organizations.

Beegerfonds, CWI
Centrum voor Wiskunde en Informatica
Koninklijke Nederlandse Akademie van Wetenschappen
Lorentz Center
Mathematical Research Institute
Rekenkamer Ludolph van Ceulen
Thomas Stieltjes Institute for Mathematics
Universiteit Leiden

Table of Contents

Invited Talks

The Complexity of Some Lattice Problems	1
<i>Jin-Yi Cai</i>	
Rational Points Near Curves and Small Nonzero $ x^3 - y^2 $ via Lattice Reduction	33
<i>Noam D. Elkies</i>	
Coverings of Curves of Genus 2	65
<i>E. Victor Flynn</i>	
Lattice Reduction in Cryptology: An Update	85
<i>Phong Q. Nguyen and Jacques Stern</i>	

Contributed Papers

Construction of Secure C_{ab} Curves Using Modular Curves	113
<i>Seigo Arita</i>	
Curves over Finite Fields with Many Rational Points Obtained by Ray Class Field Extensions	127
<i>Roland Auer</i>	
New Results on Lattice Basis Reduction in Practice	135
<i>Werner Backes and Susanne Wetzel</i>	
Baby-Step Giant-Step Algorithms for Non-uniform Distributions	153
<i>Simon R. Blackburn and Edlyn Teske</i>	
On Powers as Sums of Two Cubes	169
<i>Nils Bruin</i>	
Factoring Polynomials over p -Adic Fields	185
<i>David G. Cantor and Daniel M. Gordon</i>	
Strategies in Filtering in the Number Field Sieve	209
<i>Stefania Cavallar</i>	
Factoring Polynomials over Finite Fields and Stable Colorings of Tournaments	233
<i>Qi Cheng and Ming-Deh A. Huang</i>	
Computing Special Values of Partial Zeta Functions	247
<i>Gautam Chinta, Paul E. Gunnells, and Robert Sczech</i>	

Construction of Tables of Quartic Number Fields	257
<i>Henri Cohen, Francisco Diaz y Diaz, and Michel Olivier</i>	
Counting Discriminants of Number Fields of Degree up to Four	269
<i>Henri Cohen, Francisco Diaz y Diaz, and Michel Olivier</i>	
On Reconstruction of Algebraic Numbers	285
<i>Claus Fieker and Carsten Friedrichs</i>	
Dissecting a Sieve to Cut Its Need for Space	297
<i>William F. Galway</i>	
Counting Points on Hyperelliptic Curves over Finite Fields	313
<i>Pierrick Gaudry and Robert Harley</i>	
Modular Forms for $GL(3)$ and Galois Representations	333
<i>Bert van Geemen and Jaap Top</i>	
Modular Symbols and Hecke Operators	347
<i>Paul E. Gunnells</i>	
Fast Jacobian Group Arithmetic on C_{ab} Curves	359
<i>Ryuichi Harasawa and Joe Suzuki</i>	
Lifting Elliptic Curves and Solving the Elliptic Curve Discrete Logarithm Problem	377
<i>Ming-Deh A. Huang, Ka Lam Kueh, and Ki-Seng Tan</i>	
A One Round Protocol for Tripartite Diffie–Hellman	385
<i>Antoine Joux</i>	
On Exponential Sums and Group Generators for Elliptic Curves over Finite Fields	395
<i>David R. Kohel and Igor E. Shparlinski</i>	
Component Groups of Quotients of $J_0(N)$	405
<i>David R. Kohel and William A. Stein</i>	
Fast Computation of Relative Class Numbers of CM-Fields	413
<i>Stéphane Louboutin</i>	
On Probable Prime Testing and the Computation of Square Roots mod n .	423
<i>Siguna Müller</i>	
Improving Group Law Algorithms for Jacobians of Hyperelliptic Curves . .	439
<i>Koh-ichi Nagao</i>	
Central Values of Artin L -Functions for Quaternion Fields	449
<i>Sami Omar</i>	

The Pseudoprimes up to 10^{13}	459
<i>Richard G.E. Pinch</i>	
Computing the Number of Goldbach Partitions up to $5 \cdot 10^8$	475
<i>Jörg Richstein</i>	
Numerical Verification of the Brumer–Stark Conjecture	491
<i>Xavier-François Roblot and Brett A. Tangedal</i>	
Explicit Models of Genus 2 Curves with Split CM	505
<i>Fernando Rodriguez-Villegas</i>	
Reduction in Purely Cubic Function Fields of Unit Rank One	515
<i>Renate Scheidler</i>	
Factorization in the Composition Algebras	533
<i>Derek A. Smith</i>	
A Fast Algorithm for Approximately Counting Smooth Numbers	539
<i>Jonathan P. Sorenson</i>	
Computing All Integer Solutions of a General Elliptic Equation	551
<i>Roel J. Stroeker and Nikolaos Tzanakis</i>	
A Note on Shanks’s Chains of Primes	563
<i>Edlyn Teske and Hugh C. Williams</i>	
Asymptotically Fast Discrete Logarithms in Quadratic Number Fields	581
<i>Ulrich Vollmer</i>	
Asymptotically Fast GCD Computation in $\mathbb{Z}[i]$	595
<i>André Weilert</i>	
Author Index	615