

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 |

Algorithmic Number Theory

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

Bosma, W. (Ed.)

2000, IX, 612 p., Softcover

ISBN: 978-3-540-67695-9