

Table of Contents

Invited Talks

Gauss Composition and Generalizations	1
<i>Manjul Bhargava</i>	
Elliptic Curves — The Crossroads of Theory and Computation	9
<i>John Coates</i>	
The Weil and Tate Pairings as Building Blocks for Public Key Cryptosystems	20
<i>Antoine Joux</i>	
Using Elliptic Curves of Rank One towards the Undecidability of Hilbert's Tenth Problem over Rings of Algebraic Integers	33
<i>Bjorn Poonen</i>	
On p -adic Point Counting Algorithms for Elliptic Curves over Finite Fields	43
<i>Takakazu Satoh</i>	

Number Theory

On Arithmetically Equivalent Number Fields of Small Degree	67
<i>Wieb Bosma, Bart de Smit</i>	
A Survey of Discriminant Counting	80
<i>Henri Cohen, Francisco Diaz y Diaz, Michel Olivier</i>	
A Higher-Rank Mersenne Problem	95
<i>Graham Everest, Peter Rogers, Thomas Ward</i>	
An Application of Siegel Modular Functions to Kronecker's Limit Formula	108
<i>Takashi Fukuda, Keiichi Komatsu</i>	
Computational Aspects of NUCOMP	120
<i>Michael J. Jacobson, Jr., Alfred J. van der Poorten</i>	
Efficient Computation of Class Numbers of Real Abelian Number Fields ..	134
<i>Stéphane R. Louboutin</i>	
An Accelerated Buchmann Algorithm for Regulator Computation in Real Quadratic Fields	148
<i>Ulrich Vollmer</i>	

Arithmetic Geometry

Some Genus 3 Curves with Many Points	163
<i>Roland Auer, Jaap Top</i>	
Trinomials $ax^7 + bx + c$ and $ax^8 + bx + c$ with Galois Groups of Order 168 and $8 \cdot 168$	172
<i>Nils Bruin, Noam D. Elkies</i>	
Computations on Modular Jacobian Surfaces	189
<i>Enrique González-Jiménez, Josep González, Jordi Guàrdia</i>	
Integral Points on Punctured Abelian Surfaces	198
<i>Andrew Kresch, Yuri Tschinkel</i>	
Genus 2 Curves with $(3, 3)$ -Split Jacobian and Large Automorphism Group	205
<i>Tony Shaska</i>	
Transportable Modular Symbols and the Intersection Pairing	219
<i>Helena A. Verrill</i>	

Elliptic Curves and CM

Action of Modular Correspondences around CM Points	234
<i>Jean-Marc Couveignes, Thierry Henocq</i>	
Curves $Dy^2 = x^3 - x$ of Odd Analytic Rank	244
<i>Noam D. Elkies</i>	
Comparing Invariants for Class Fields of Imaginary Quadratic Fields	252
<i>Andreas Enge, François Morain</i>	
A Database of Elliptic Curves – First Report	267
<i>William A. Stein, Mark Watkins</i>	

Point Counting

Isogeny Volcanoes and the SEA Algorithm	276
<i>Mireille Fouquet, François Morain</i>	
Fast Elliptic Curve Point Counting Using Gaussian Normal Basis	292
<i>Hae Young Kim, Jung Youl Park, Jung Hee Cheon, Je Hong Park, Jae Heon Kim, Sang Geun Hahn</i>	
An Extension of Kedlaya's Algorithm to Artin-Schreier Curves in Characteristic 2	308
<i>Jan Denef, Frederik Vercauteren</i>	

Cryptography

Implementing the Tate Pairing	324
<i>Steven D. Galbraith, Keith Harrison, David Soldera</i>	
Smooth Orders and Cryptographic Applications	338
<i>Carl Pomerance, Igor E. Shparlinski</i>	
Chinese Remaindering for Algebraic Numbers in a Hidden Field	349
<i>Igor E. Shparlinski, Ron Steinfeld</i>	

Function Fields

An Algorithm for Computing Weierstrass Points	357
<i>Florian Hess</i>	
New Optimal Tame Towers of Function Fields over Small Finite Fields ...	372
<i>Wen-Ching W. Li, Hiren Maharaj, Henning Stichtenoth, Noam D. Elkies</i>	
Periodic Continued Fractions in Elliptic Function Fields	390
<i>Alfred J. van der Poorten, Xuan Chuong Tran</i>	

Discrete Logarithms and Factoring

Fixed Points and Two-Cycles of the Discrete Logarithm	405
<i>Joshua Holden</i>	
Random Cayley Digraphs and the Discrete Logarithm	416
<i>Jeremy Horwitz, Ramarathnam Venkatesan</i>	
The Function Field Sieve Is Quite Special	431
<i>Antoine Joux, Reynald Lercier</i>	
MPQS with Three Large Primes	446
<i>Paul Leyland, Arjen Lenstra, Bruce Dodson, Alec Muffett, Sam Wagstaff</i>	
An Improved Baby Step Giant Step Algorithm for Point Counting of Hyperelliptic Curves over Finite Fields	461
<i>Kazuto Matsuo, Jinhui Chao, Shigeo Tsujii</i>	
Factoring $N = pq^2$ with the Elliptic Curve Method	475
<i>Peter Ebinger, Edlyn Teske</i>	

Gröbner Bases

A New Scheme for Computing with Algebraically Closed Fields	491
<i>Allan Steel</i>	

Complexity

Additive Complexity and Roots of Polynomials
over Number Fields and \mathfrak{p} -adic Fields 506
 J. Maurice Rojas

Author Index 517

Algorithmic Number Theory

5th International Symposium, ANTS-V, Sydney, Australia,

July 7-12, 2002. Proceedings

Fieker, C.; Kohel, D.R. (Eds.)

2002, X, 522 p., Softcover

ISBN: 978-3-540-43863-2