

# Table of Contents

## Invited Talks

Computing Zeta Functions via $p$ -Adic Cohomology . . . . .	1
<i>Kiran S. Kedlaya</i>	
Using Primitive Subgroups to Do More with Fewer Bits . . . . .	18
<i>K. Rubin, A. Silverberg</i>	
Elliptic Curves of Large Rank and Small Conductor . . . . .	42
<i>Noam D. Elkies, Mark Watkins</i>	

## Contributed Papers

Binary GCD Like Algorithms for Some Complex Quadratic Rings . . . . .	57
<i>Saurabh Agarwal, Gudmund Skovbjerg Frandsen</i>	
On the Complexity of Computing Units in a Number Field . . . . .	72
<i>V. Arvind, Piyush P. Kurur</i>	
Implementing the Arithmetic of $C_{3,4}$ Curves . . . . .	87
<i>Abdolali Basiri, Andreas Enge, Jean-Charles Faugère, Nicolas Gürel</i>	
Pseudocubes and Primality Testing . . . . .	102
<i>P. Berrizbeitia, S. Müller, H.C. Williams</i>	
Elliptic Curves with a Given Number of Points . . . . .	117
<i>Reinier Bröker, Peter Stevenhagen</i>	
Rational Divisors in Rational Divisor Classes . . . . .	132
<i>N. Bruin, E.V. Flynn</i>	
Conjectures about Discriminants of Hecke Algebras of Prime Level . . . . .	140
<i>Frank Calegari, William A. Stein</i>	
Montgomery Scalar Multiplication for Genus 2 Curves . . . . .	153
<i>Sylvain Duquesne</i>	
Improved Weil and Tate Pairings for Elliptic and Hyperelliptic Curves . . . . .	169
<i>Kirsten Eisenträger, Kristin Lauter, Peter L. Montgomery</i>	
Elliptic Curves $x^3 + y^3 = k$ of High Rank . . . . .	184
<i>Noam D. Elkies, Nicholas F. Rogers</i>	

Proving the Primality of Very Large Numbers with fastECPP . . . . .	194
<i>J. Franke, T. Kleinjung, F. Morain, T. Wirth</i>	
A Low-Memory Parallel Version of Matsuo, Chao, and Tsuji's Algorithm . . . . .	208
<i>Pierrick Gaudry, Éric Schost</i>	
Function Field Sieve in Characteristic Three . . . . .	223
<i>R. Granger, A.J. Holt, D. Page, N.P. Smart, F. Vercauteren</i>	
A Comparison of CEILIDH and XTR . . . . .	235
<i>R. Granger, D. Page, M. Stam</i>	
Stable Models of Elliptic Curves, Ring Class Fields, and Complex Multiplication . . . . .	250
<i>Jordi Guàrdia, Eugenia Torres, Montserrat Vela</i>	
An Algorithm for Computing Isomorphisms of Algebraic Function Fields . . . . .	263
<i>F. Hess</i>	
A Method to Solve Cyclotomic Norm Equations $f * \bar{f}$ . . . . .	272
<i>Nick Howgrave-Graham, Mike Szydło</i>	
Imaginary Cyclic Quartic Fields with Large Minus Class Numbers . . . . .	280
<i>M.J. Jacobson, Jr., H.C. Williams, K. Wooding</i>	
Nonic 3-adic Fields . . . . .	293
<i>John W. Jones, David P. Roberts</i>	
Montgomery Addition for Genus Two Curves . . . . .	309
<i>Tanja Lange</i>	
Numerical Evaluation at Negative Integers of the Dedekind Zeta Functions of Totally Real Cubic Number Fields . . . . .	318
<i>Stéphane R. Louboutin</i>	
Salem Numbers of Trace $-2$ and Traces of Totally Positive Algebraic Integers . . . . .	327
<i>James McKee, Chris Smyth</i>	
Low-Dimensional Lattice Basis Reduction Revisited . . . . .	338
<i>Phong Q. Nguyen, Damien Stehlé</i>	
Computing Order Statistics in the Farey Sequence . . . . .	358
<i>Corina E. Pătraşcu, Mihai Pătraşcu</i>	
The Discrete Logarithm in Logarithmic $l$ -Class Groups and Its Applications in K-theory . . . . .	367
<i>Sebastian Pauli, Florence Soriano-Gafiuk</i>	

Point Counting on Genus 3 Non Hyperelliptic Curves . . . . .	379
<i>Christophe Ritzenthaler</i>	
Algorithmic Aspects of Cubic Function Fields . . . . .	395
<i>R. Scheidler</i>	
A Binary Recursive Gcd Algorithm . . . . .	411
<i>Damien Stehlé, Paul Zimmermann</i>	
Lagrange Resolvents Constructed from Stark Units . . . . .	426
<i>Brett A. Tangedal</i>	
Cryptanalysis of a Divisor Class Group Based Public-Key Cryptosystem . . . . .	442
<i>Aaram Yun, Jaeheon Kim, Dong Hoon Lee</i>	
<b>Author Index</b> . . . . .	451



<http://www.springer.com/978-3-540-22156-2>

Algorithmic Number Theory

6th International Symposium, ANTS-VI, Burlington, VT,  
USA, June 13-18, 2004, Proceedings

Buell, D. (Ed.)

2004, XII, 456 p., Softcover

ISBN: 978-3-540-22156-2