Invited and Submitted Talks ANTS IV

Invited Talks

Frits Beukers, *A rational approach to* π

Peter Borwein, *The 40 trillionth binary digit of* π *is 0*

Jin Yi Cai, *The Complexity of Some Lattice Problems*

Noam Elkies, *Points near Curves*

Victor Flynn, *Coverings of Curves of Genus 2*

Phong Q. Nguyen, Jacques Stern, *Lattice Reduction in Cryptology: an Update*

Submissions

Seigo Arita, *Construction of Secure* C_{ab} *Curves Using Modular Curves*

Roland Auer, *Curves over Finite Fields with Many Rational Points Obtained by Ray Class Field Extensions*

Werner Backes, Susanne Wetzel, *New Results on Lattice Basis Reduction in Practice*

Simon R. Blackburn, Edlyn Teske, *Baby-Step Giant-Step Algorithms for Non-Uniform Distributions*

Nils Bruin, *On powers as sums of two cubes*

David G. Cantor, Daniel M. Gordon, *Factoring polynomials over* $\mathbf{Q}_p$

Stefania Cavallar, *Strategies in Filtering in the Number Field Sieve*

Qi Cheng, Ming-Deh A. Huang, *Factoring Polynomials over Finite Fields and Stable Colorings of Tournaments*

Gautam Chinta, Paul E. Gunnells, Robert Sczech, *Computing special values of partial zeta functions*

Henri Cohen, Francisco Diaz y Diaz and Michel Olivier, *Counting discriminants of number fields*

Henri Cohen, Francisco Diaz y Diaz and Michel Olivier, *Construction of tables of quartic number fields*

Claus Fieker and Carsten Friedrichs, *On Reconstruction of Algebraic Numbers*

William F. Galway, *Dissecting a sieve to cut its need for space*

Pierrick Gaudry, Robert Harley, *Counting Points on Hyperelliptic Curves over Finite Fields*

Bert van Geemen, Jaap Top, *Modular Forms for* GL(3) *and Galois Representations*

Paul E. Gunnells, *Modular symbols and Hecke operators*

Ryuichi Harasawa, Joe Suzuki, *Fast Implementation of Jacobian Group Arithmetic on* C_{ab} *Curves*

Ming-Deh A. Huang, Ka Lam Kueh, Ki-Seng Tan, *Lifting Elliptic Curves and Solving Elliptic Curve Discrete Logarithm Problem*

Antoine Joux, *A one round protocol for tripartite Diffie–Hellman*

David R. Kohel, Igor E. Shparlinski, *On Exponential Sums and Group Generators for Elliptic Curves over Finite Fields*

David Kohel, William A. Stein, *Component Groups of Quotients of* $J_0(N)$

Stéphane Louboutin, *Fast computation of relative class numbers of CM-fields*

Siguna Müller, *On Probable Prime Testing and the Computation of Square Roots* $\bmod n$

Koh-ichi Nagao, *Some Improvements of Computing Jacobian of Hyper Elliptic Curve*

Sami Omar, *Central Values of Artin L-Functions of the Quaternion Fields*

Richard G.E. Pinch, *The pseudoprimes up to* 10^{13}

Jörg Richstein, *Computing the Number of Goldbach Partitions up to* $5 \cdot 10^8$

Xavier-François Roblot, Brett A. Tangedal, *Numerical Verification of the Brumer-Stark Conjecture*

Fernando Rodriguez-Villegas, *Explicit model of genus 2 curves with split CM*

Derek A. Smith, *Factorization in the Maximal Arithmetics of the Composition Algebras*

Jonathan P. Sorenson, *A Fast Algorithm for Approximately Counting Smooth Numbers*

R.J. Stroeker, N. Tzanakis, *Computing all integer solutions of a general elliptic equation*

E. Teske, H. C. Williams, *A note on Shanks's Chains of Primes*

Ulrich Vollmer, *Asymptotically Fast Discrete Logarithms in Quadratic Number Fields*

André Weilert, *Asymptotically Fast GCD Computation in* $\mathbf{Z}[i]$