Algorithms and Number Theory

Programme

Monday, 25.5.2009

10:00 - 10:45 M. Stoll: Rational points on curves of genus 2: Experiments and speculations

11:00 - 11:45 P. Stevenhagen: Constructing genus 2 curves and Jacobians of given order

16:00 - 16:40 R. Scheidler: Construction of all cubic function fields of fixed, even degree discriminant

16:50 - 17:20 A. Morra: An algorithm to compute relative cubic fields

17:30 - 18:00 M. Jacobson: Tabulating class groups of quadratic fields

Tuesday, 26.5.2009

09-15 - 10:00 D. Bernstein: Code-based post quantum cryptography

10:20 - 10:50 R. Lindner: Density of ideal lattices

11:00 - 11:30 M. Rückert: Lattice-based blind signatures

11:40 - 12:10 M. Schneider: Probabilistic analysis of LLL-reduced bases

16:00 - 16:30 W. B. Hart: FLINT: A fast library for number theory

16:40 - 17:10 B. Allombert: A new GP interpreter

17:20 - 17:50 O. Uzunkol: The SCIEnce project

Wednesday, 27.5.2009

09-15 - 10:00 B. de Smit: Standard models of finite fields

10:30 - 11:00 M. Rückert: www.latticechallenge.org

11:10 - 11:50 S. Pauli: Zero-free regions for the derivatives of the Riemann zeta functions

Thursday, 28.5.2009

09-15 - 10:00 R. Bradshaw: Sage - a platform for computational number theory

10:30 - 11:00 A. Enge: CM - Software for complex multiplication

11:10 - 11:55 S. Donnelly: New developments in Magma

15:50 - 16:30 O. Uzunkol: Theta functions, class units and some applications

16:40 - 17:10 D. Kohel: CM invariants in dimension 2

17:20 - 17:50 R. L. Miller: An algorithm for proving BSD

Friday, 29.5.2009

09:30 - 10:00 F. Hess: Pairings from small degree functions

10:20 - 10:50 T. Lange: Pairings on Edwards curves

11:00 - 11:30 K. Nakamula: On imaginary quadratic quantum public key cryptosystems