London Mathematical Society Durham Symposium
on
COMPUTATIONAL NUMBER THEORY

PROGRAMME OF LECTURES

MONDAY 24 JULY		
2.00 p.m. - 7.00 p.m.		***Conference Registration (Holgate House, Grey College)***
4.00 p.m. - 7.00 p.m.		Tea and coffee: Seminar Room 1, Holgate House, Grey College
7.00 p.m.		Dinner (Main Dining Hall, Grey College)
TUESDAY 25 JULY		
9.00 a.m.	*G. Frey*	Height Conjectures and Galois Representations Attached to Elliptic Curves
10.00 a.m.	*V. Shoup*	Provable security
11.10 a.m. - 11.40 a.m.		*Coffee Break (CM103/CM105, Mathematical Sciences)*
11.45 a.m.	*H. Cohen*	Explicit construction of number field extensions of small degree, with applications to discriminant counting I
1.00 p.m.		*Lunch (Main Dining Hall, Grey College)*
3.30 p.m.		*Tea Break (CM103/CM105, Mathematical Sciences)*
4.00 p.m.	*S. Galbraith*	Elliptic Curve Cryptography and Weil descent I
5.00 p.m.	*N.P.Smart*	Elliptic Curve Cryptography and Weil descent II
6.30 p.m.		***Sherry Reception (JCR, Grey College)***
7.00 p.m.		*Dinner (Main Dining Hall, Grey College)*

WEDNESDAY 26 JULY		
9.00 a.m.	*F. Morain*	Modular Curves and Class Invariants
10.00 a.m.	*R. Schoof*	Abelian varieties over number fields with good reduction everywhere
11.10 a.m. - 11.40 a.m		*Coffee Break (CM103/CM105, Mathematical Sciences)*
11.45 a.m.	*A. Van der Poorten*	An introduction to NUCOMP
1.00 p.m.		*Lunch (Main Dining Hall, Grey College)*
3.30 p.m.		*Tea Break (CM103/CM105, Mathematical Sciences)*
4.00 p.m.	*M. Stoll*	Reduction of binary forms - how to find small equations for hyperelliptic curves
4.45 p.m.	*C.J. Smyth*	Finding torsion cosets on hypersurfaces
5.30 p.m.	*W.A. Stein*	Shafarevich-Tate groups of modular abelian varieties
7.00 p.m.		*Dinner (Main Dining Hall, Grey College)*
THURSDAY 27 JULY		
9.00 a.m.	*D.J. Bernstein*	Rethinking the number field sieve
10.00 a.m.	*H. Cohen*	Explicit construction of number field extensions of small degree, with applications to discriminant counting II
11.10 a.m. - 11.40 a.m.		*Coffee Break - CM103/CM105 (Mathematical Sciences)*
11.45 a.m.	*J. Cannon*	Arithmetic Geometry in Magma
1.00 p.m.		*Lunch (Main Dining Hall, Grey College)*
2.00 p.m.		***Conference Group Photograph (Grey College Steps)***
2.40 p.m.		***Cathedral Visit***
7.00 p.m.		Dinner (Main Dining Hall, Grey College)

FRIDAY 28 JULY		
9.00 a.m.	*H. C. Williams*	A key exchange protocol based on real quadratic fields
10.00 a.m.	*D. Hühnlein*	Imaginary quadratic orders and cryptography
11.10 a.m. - 11.40 a.m.		*Coffee Break - CM103/CM105 (Mathematical Sciences)*
11.45am	*M. Jacobson*	Non-interactive public key cryptography using non-maximal imaginary quadratic orders
1.00 p.m.		*Lunch (Main Dining Hall, Grey College)*
3.30 p.m.		*Tea Break (CM103/CM105, Mathematical Sciences)*
4.00pm	*N.P.Smart*	Elliptic Curve Cryptography and Weil descent III
4.45pm	*S. Galbraith*	Elliptic Curve Cryptography and Weil descent IV
5.30pm	*A. Petho*	S-integral points on elliptic curves
7.00 p.m.		Dinner (Main Dining Hall, Grey College)
SATURDAY 29 JULY		
9.00 a.m.	*S. Gao*	A new method for factoring multivariate polynomials via partial differential equations
10.00 a.m.	*A. Lauder*	Fast absolute irreducibility testing for sparse polynomials
11.10 a.m.		*Coffee Break - CM103/CM105 (Mathematical Sciences)*
11.45 a.m.	*D. Ford*	Polynomial factorization over p-adic fields
1.00 p.m.		*Lunch (Holgate House, Grey College)*
7.00 p.m.		*Dinner (Main Dining Hall, Grey College)*
SUNDAY 30 JULY		
9.15 a.m.		**Day Trip - Whitby and Robin Hood's Bay (see separate programme)**
7.00 p.m.		*Dinner (Main Dining Hall, Grey College)*

MONDAY 31 JULY		
9.00 a.m.	*R. Scheidler*	Function fields and cryptography
10.00 a.m.	*J.H. Davenport*	Recent Developments in Cryptography: What is "breaking RSA"
11.10 a.m.		*Coffee Break - CM103/CM105 (Mathematical Sciences)*
11.45 a.m.	*E. Teske*	The parallelized Pollard Kangaroo method in real quadratic function fields
1.00 p.m.		*Lunch (Holgate House, Grey College)*
3.30 p.m.		*Tea Break (CM103/CM105, Mathematical Sciences)*
4.00 p.m.	*B. H. Matzat*	Iterative differential equations and Abhyankar's Conjecture
5.00 p.m.	*B. de Smit*	The interactive group theory of arithmetically equivalent fields
7.00 p.m.		*Dinner (Main Dining Hall, Grey College)*
TUESDAY 1 AUGUST		
9.00 a.m.	*C. Schnorr*	Practical lattice basis reduction in high dimensions
10.00 a.m.	*T. Fisher*	Estimating the rank of an elliptic curve over its field of n-division points
11.10 a.m. - 11.40 a.m.		*Coffee Break (CM103/CM105, Mathematical Sciences)*
11.45 a.m.	*J. Klüners*	Constructive Galois Theory
1.00 p.m.		*Lunch (Holgate House, Grey College)*
3.30 p.m. - 4.00 p.m.		*Tea Break (CM103/CM105, Mathematical Sciences)*
4.00 p.m.	*M. Watkins*	Real zeros of real odd Dirichlet L-functions and class numbers of imaginary quadratic fields
4.45 p.m.	*M. Maurer*	Finding a generating unit by real-gcd computations
5.30 p.m.	*J. McKee*	Little by little lattice reduction and integer factorization
7.00 p.m.		***Sherry Reception (JCR, Grey College)***
7.30 p.m.		***Conference Dinner (Main Dining Hall, Grey College)***

WEDNESDAY 2 AUGUST		
9.00 a.m.	*E.V. Flynn*	Fermat quartics and a challenge curve of Serre
10.00 a.m.	*N. Bruin*	Finding rational points on curves of genus 3
11.10 a.m. - 11.40 a.m.		*Coffee Break (CM103/CM105, Mathematical Sciences)*
11.45 a.m.	*J.-M. Couveignes*	Coverings of algebraic curves : explicit methods and applications
1.00 p.m.		*Lunch (Holgate House, Grey College)*
3.30 p.m. - 4.00 p.m.		*Tea Break (CM103/CM105, Mathematical Sciences)*
4.00 p.m.	*P. Gaudry*	Schoof's algorithm in genus 2
5.00 p.m.	*B.J. Birch*	40 years on
THURSDAY 3 AUGUST		
Breakfast to be taken in the Main Dining Hall, Grey College		