Future directions in algorithmic number theory

Workshop Schedule

Monday, March 24, 2003
9:15 am - Manindra Agrawal: A polynomial time for testing primality
11:00 am - Hendrik W. Lenstra, Jr.: Primality testing with pseudofields
Lunch
2:30 pm - Alan Lauder: Counting solutions to equations in many variables over finite fie
4:00 pm - Bas Edixhoven: About pont counting over arbitrary finite fields
5:10 pm - Manindra Agrawal: Finding quadratic nonresidues
5:50 pm - Brainstorming session [Moderated by Jonathan Pila]

Tuesday, March 25, 2003
9:00 am - Carl Pomerance and Daniel Bleichenbacher: Constructing finite fields
10:45 am - Felipe Voloch: Subgroups of (Fq[x]/(h))*
11:30 am - Problem session [Moderated by Jonathan Pila]
Lunch
2:00 pm - Pedro Berrizbeitia: Sharpening AKS for a large family of numbers
2:45 pm - Qi Cheng: Primality proving via one round in ECPP and one iteration in AKS
3:45 pm - Daniel Bernstein: Randomized primality proving in essentially quartic time

Wednesday, March 26, 2003
9:00 am - Alice Silverberg: Applications of algebraic tori to cryptography
10:45 am - Arjen Lenstra: Factoring integers
11:30 am - Daniel Bernstein: Rethinking the Number Field Sieve-an update
Afternoon hike!

Thursday, March 27, 2003
9:00 am - Daqing Wan: Partial counting of rational points over finite fields
10:45 am - Jean-Marc Couveignes
11:30 am - Mark Watkins: Computing the number of points on a curve
Lunch
2:00 pm - Kiran Kedlaya: Counting points using p-adic cohomology
3:00 pm - William Stein: The modular forms database project
4:00 pm - Problem session [Moderated by Peter Stevenhagen]

Friday, March 28, 2003
9:00 am - Siguna Mueller: an efficient method for recognising industrial-grade primes
9:25 am - Preda Mihailescu: Practical AKS?!
9:50 am - Rene Schoof: Cohen/Lenstra Heuristics
10:45 am - Problem session in working groups
Lunch

2:00 pm - Shuhong Gao: Deterministic factoring under GRH
2:45 pm - Victor Shoup: Kalai's algorithm for generating random factored integers
3:45 pm - Problem session [Moderated by Michael Zieve]
5:00 pm - Dan Goldston: Small gaps between consecutive primes
6:00 pm - Reception