Future directions in algorithmic number theory

organized by
Hendrik Lenstra, Carl Pomerance, and Jonathan Pila

Workshop Summary

The workshop was organized in response to the "Primes in P" result. In the late summer of 2002, Agrawal, Kayal, and Saxena (AKS) found a simple deterministic polynomial time algorithm which determines whether or not an integer is prime. This result opened the possibility that there may be similar problems which could be attacked by such methods (most significantly, it is remotely possible that similar ideas could lead to a way to factor integers.) This workshop was quickly organized, and its purpose was to completely understand the AKS algorithm and to explore other problems in that theme.

The workshop began with talks on the AKS algorithm: recent refinements and the possibilities for improvements. The remaining talks primarily concerned algorithms over finite fields. In addition, four problem sessions explored open questions for future work (see the AIM website for more details).

A main theme of the workshop was the possibility of improvements to the AKS algorithm. At the end of the first day Agrawal described an approach to the problem of finding square roots over finite fields in polynomial time. The algorithm rested on a conjecture which, if correct, would also give a significant improvement in the AKS algorithm.

Lenstra and Pomerance led an extensive discussion on Agrawals conjecture, and they were strongly of the opinion that the conjecture is false. An outline of a heuristic argument was given.