

*Department of Mathematics,
University of California, San Diego*

Math 209 - Number Theory Seminar

Reinier Broker

Microsoft

A fast multi-prime approach to compute the Hilbert class polynomial

Abstract:

The computation of the Hilbert class polynomial has applications ranging from explicit class field theory to cryptography. Several new algorithms to compute it have been developed during the last 5 years, each having its pro's and cons. In this talk we will present a significant speed up of the 'Chinese remainder theorem approach'. We will give a detailed run time analysis of the new algorithm, using tools from both analytic number theory and arithmetic geometry. The resulting run time is almost optimal: one of the bottlenecks is writing down the answer.

Host: Kristen Lauter

Thursday, May 8, 2008

2:00 PM

AP&M 7421
