N16

Colloquium

On the complexity of factoring polynomials over finite fields

Kiran Kedlaya

Abstract: Abstract: While factoring large polynomials over finite fields is (apparently) far easier than factoring large integers, it is still an open problem to give an algorithm that does it "as fast as possible" (roughly speaking, in time proportional to the length of the input data). We will explain a recent improvement in the complexity of factoring polynomials over finite fields, based on an asymptotically optimal solution of a related problem (the modular composition problem). Joint work with Chris Umans (Caltech).

Tuesday, February 24, 2009, 4:00 pm
Mathematics and Science Center: W201

Mathematics and Computer Science
Emory University