Sieving in Number Field Sieve

21 March, 2018

Abstract:

Number Field Sieve(NFS) is the fastest known algorithm for factoring integers larger than 100 digits. In this talk, I present an in-depth analysis of the Sieving step of NFS, emphasizing on the technique of Lattice Sieving along with a small implementation of it.

Swati
Research Assistant- 1
Supervisor: Dr. Ben Kane
Department of Mathematics
HKU