An Implementation of the Number Field Sieve

Marije Elkenbracht-Huizing

Abstract

The Number Field Sieve (NFS) is the asymptotically fastest known factoring algorithm for large integers. This article describes an implementation of the NFS, including the choice of two quadratic polynomials, both classical sieving and a special form of lattice sieving (line sieving), the block Lanczos method and a new square root algorithm. Finally some data on factorizations obtained with this implementation are listed, including the record factorization of $12^{151} - 1$.