Title: Supporting algorithms of number field sieve

Author: Adéla Skoková

Department: Department of Algebra

Supervisor: prof. RNDr. Aleš Drápal, CSc., DSc.

Abstract:
In this work we study the first part of the algorithm of number field sieve, generating of polynomials. At first we describe all the algorithm of the sieve for understanding of the role of polynomials and their impact on the entire algorithm. Then we present their characteristics and evaluation. The last part is about the most effective know algorithms of generating polynomials, invented by Thorsen Klinjung. The second Kleinjung algoritm was also programmed.

Keywords:
GNFS, Number sieve, Number field, Kleinjung algorithm