Title: Generating polynomials for number field sieve

Author: Anežka Pejlová

Department: Department of Algebra

Supervisor: prof. RNDr. Aleš Drápal, CSc., DSc., Department of Algebra

Abstract: The topic of this thesis is mainly focused on Kleinjung algorithm for generating polynomials within the General Number Field Sieve, which is the most efficient factorization algorithm nowadays. Commonly used consecutions are explained with respect to the fact whether they can be rigorously proven or they are based only on heuristic assumptions. Another contribution of this thesis is the attached implementation of Kleinjung algorithm developed as a part of the Number Field Sieve project led by the Department of Algebra. The appropriateness of some heuristics used in the theory beyond the Kleinjung algorithm is supported by empirical data obtained from this implementation.

Keywords: Number field sieve, Kleinjung algorithm