Název práce: Generování polynomů pro číselné síto

Autor: Anežka Pejlová

Katedra: Katedra algebry

Vedoucí diplomové práce: prof. RNDr. Aleš Drápal, CSc., DSc., Katedra algebry

Abstrakt: V této práci se zaměřujeme zejména na Kleinjungův algoritmus pro generování polynomů v rámci obecného číselného síta, což je v současnosti nejefektivnější faktorizační algoritmus. Obecně užívané postupy jsou popsány s důrazem na vysvětlení, které části lze rigorózně dokázat a které jsou motivovány pouze heuristicky. Přínosem práce je také přiložená implementace Kleinjungova algoritmu vyvinutá v rámci projektu NFS vedeného na Katedře algebry. Empirická data získaná z této implementace podpírají vhodnost některých popsaných heuristik.

Klíčová slova: Číselné síto, Kleinjungův algoritmus