

Název práce: Podpůrné algoritmy číselného síta

Autor: Adéla Skoková

Katedra: Katedra algebry

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

Abstrakt: V předložené diplomové práci studujeme hlavně první fázi algoritmu číselného síta, generování polynomů. Nejprve popisujeme celé číselné síto pro pochopení role polynomů a jejich vliv na celý algoritmus. Pak se věnujeme jejich vlastnostem a ohodnocování. Nakonec uvádíme algoritmy pro generování polynomů, se kterými přišel Thorsen Kleinjung. Druhý Kleinjungův algoritmus byl naprogramován. Jedná se o zatím nepřekonané algoritmy na získávání vhodných polynomů.

Klíčová slova:

Číselné síto, GNFS, Číselné těleso, Kleinjungův algoritmus