Název práce: Faktorizace polynomů nad konečnými tělesy

Autor: Milan Straka

Katedra (ústav): Katedra algebry

Vedoucí bakalářské práce: Mgr. Jan Žemlička, Ph.D.

E-mail vedoucího: *Jan.Zemlicka@mff.cuni.cz*

Abstrakt: Cílem práce je prozkoumat problém rozkladu polynomu nad konečným tělesem na součin ireducibilních polynomů. Popsáním několika algoritmů hledajících tento rozklad se ukáže, že tento problém je vždy řešitelný v polynomiálním čase vzhledem ke stupni polynomu a počtu prvků konečného tělesa.

U jednoho z algoritmů je popsána implementace s velmi dobrou asymptotickou časovou složitostí $\mathcal{O}(n^{1.815} \log q)$, kde n je stupeň rozkládaného polynomu nad tělesem s q prvky. Program používající jednodušší, ale prakticky rychlejší variantu tohoto algoritmu je součástí práce.

Klíčová slova: faktorizace, konečná tělesa, polynomy, algoritmus

Title: Factoring polynomials over finite fields

Author: Milan Straka

Department: Department of Algebra

Supervisor: Mgr. Jan Žemlička, Ph.D.

Supervisor's e-mail address: *Jan.Zemlicka@mff.cuni.cz*

Abstract: The goal of this work is to present the problem of the decomposition of a polynomial over a finite field into a product of irreducible polynomials. By describing algorithms solving this problem, we show that the decomposition can always be found in polynomial time in both the degree of the polynomial and the number of elements of the underlying finite field.

One algorithm is studied in detail and an implementation with good asymptotic time complexity $\mathcal{O}(n^{1.815} \log q)$ is described, where n is the degree of the polynomial over the field with q elements. A program using easier, but practically faster version of this algorithm is a part of this work.

Keywords: factorization, finite fields, polynomials, algorithm