Povzetek

V tem delu bomo definirali baze binarnih končnih obsegov, ki se v kriptografiji nad eliptičnimi krivuljami uporabljajo najpogosteje. To so polinomske, normalne in sebidualne baze. Pri polinomskih bazah bomo posebej obravnavali tiste, ki imajo za redukcijski polinom trinom ali pentonom. Pri normalnih bazah pa bomo definirali posebni vrsti baz, to so optimalne normalne in umbralne baze. Glede na različne baze bomo podali najhitrejše algoritme za osnovne operacije; to so seštevanje, množenje, kvadriranje in računanje inverza. Naredili bomo podrobno analizo algoritmov in primerjavo med njimi. Poleg tega bomo predstavili algebraične osnove končnih obsegov in eliptičnih krivulj, ki so pomembne za javno kriptografijo z eliptičnimi krivuljami.

Ključne besede: Eliptične krivulje, polinomske baze, normalne baze, optimalne normalne baze, umbralne baze, sebidualne baze, končni obsegi.

Abstract

In this thesis we will define bases for binary finite fields, which are most common in elliptic curve cryptography. These are polynomial, normal and self-dual bases. We will concentrate on those polynomial bases, that are defined with irreducible trinomial or pentonomial. Also two special kind of normal bases will be defined, optimal normal bases and umbral bases. We will describe the fastest algorithms for basic operations in different bases; these are addition, multiplication, squaring and inversion. We will make a detailed analysis of these algorithms and their comparison. We will also introduce some basics about finite fields and elliptic curves, which are of particular interest to public criptography with elliptic curves.

Key words: Elliptic curves, polynomial bases, normal bases, optimal normal bases, umbral bases, self-dual bases, finite fields.

Math. subj. class (2003): 11G05, 11T71, 11Y16, 14H52, 68W30, 68Q65.

Literatura

[1] I. Vidav, *Algebra*, Mladinska knjiga, Ljubljana, 1989.

[2] Lidl, Niederreiter, *Finite fields*, Cambridge University Press, 1987.

[3] D. Hankerson, J.Lopez Hernandez, A. Menezes, *Software Implementation of Elliptic Curve Cryptography Over Binary Fields*, University of Waterloo, Faculty of Mathematics,CORR 2000-42 (Avgust 2000).

[4] A. Menezes, I. A. Blake, X. Gao, R. C. Mullin, S. A. Vanstone, T. Yaghoobian, *Applications of Finite Fields*, Kluwer Academic Publishers, 1992.

[5] A. Jurišić, *Umbral optimal normal bases*, Politehnika Nova Gorica in IMFM (Avgust 2001).

[6] A. Menezes, *Elliptic Curve Public Key Cryptosystems*, Kluwer Academic Publishers, 1993.