МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ

Кафедра высшей алгебры и защиты информации

ЦИВАКО

Дарья Сергеевна

МЕТОДЫ ФАКТОРИЗАЦИИ МНОГОЧЛЕНОВ НАД КОНЕЧНЫМИ ПОЛЯМИ

Дипломная работа

Научный руководитель:
доктор физико-математических наук,
профессор В.В. Беняш-Кривец

Допущена к защите

«___» _____ 2022 г.

Зав. кафедрой высшей алгебры и защиты информации

доктор физико-математических наук, профессор В.В. Беняш-Кривец

Минск, 2022

РЕФЕРАТ

Дипломная работа: 41 с., 5 источников.

Ключевые слова: наибольший общий делитель, неприводимый многочлен, бесквадратный многочлен, f-разлагающий многочлен, алгоритм Кантора—Цассенхауза, примитивный многочлен.

Объект исследования: многочлены над конечными полями и их факторизация.

Цель исследования: изучение методов факторизации многочленов над конечными полями.

Полученные результаты: были изучены методы факторизации многочленов над конечными полями, описаны алгоритмы для каждого из этапов факторизации и даны оценки для каждого из алгоритмов.

Автор работы подтверждает, что приведенный в ней расчетноаналитический материал правильно и объективно отражает состояние исследуемого процесса, а все заимствованные из литературных и других источников теоретические, методологические и методические положения и концепции сопровождаются ссылками на их авторов.

РЭФЕРАТ

Дыпломная праца: 41 с., 5 крыніц.

Ключавыя словы: найбольшы агульны дзельнік, непрыводны мнагачлена, бесквадратны мнагачлена, f- раскладальны мнагачлена, алгарытм Кантора-Цассенхауза, прымітыўны мнагачлена.

Аб'ект даследавання: мнагачлены над канчатковымі палямі і іх факторызацыя.

Цэль даследавання: вывучэнне метадаў фактарызацыі мнагачленаў над канечнымі палямі.

Атрыманыя вынікі: былі вывучаны метады факторызацыі мнагачлена над канчатковымі палямі, апісаны алгарытмы для кожнага з этапаў факторызацыі і дадзены ацэнкі для кожнага з алгарытмаў.

Аўтар працы пацвярджае, што прыведзены ў èй разлікова-аналітычны матэрыял правільна і аб'ектыўна адлюстроўвае стан доследнага працэсу, а ўсе запазычаныя з літаратурных і іншыхкрыніц тэарэтычныя, метадалагічныя і метадычныя становішча і канцэпцыі суправаджаюцца спасылкамі на іх аўтараў.

ANNOTATION

Degree paper: 41 p., 5 sources.

Keywords: greatest common divisor, irreducible polynomial, squareless polynomial, f-splitting polynomial, Cantor–Zassenhaus algorithm, primitive polynomial.

Object of research: polynomials over finite fields and their factorization.

Purpose of research: the research of methods for factorization of polynomials over finite fields.

Obtained results: Methods for factorization of polynomials over finite fields were researched, algorithms for each of the factorization stages were described, and estimates were given for each of the algorithms.

The author of the work confirms that computational and analytical material presented in it correctly and objectively reproduces the picture of investigated process, and all the theoretical, methodological and methodical positions and concepts borrowed from literary and other sources are given references to their authors.