БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ

Кафедра дифференциальных уравнений и системного анализа

Аннотация к дипломной работе

АЛГЕБРАИЧЕСКИЕ УРАВНЕНИЯ НАД ПОЛЯМИ ГАЛУА

Барышева Анастасия Андреевна

Научный руководитель:
Профессор, доктор техн. наук В.А. Липницкий

2017

В дипломной работе 56 страниц, 5 таблиц, 13 источников, 5 приложений.

Ключевые слова: АЛГЕБРАИЧЕСКИЕ УРАВНЕНИЯ, ПОЛЯ ГАЛУА, ФОРМУЛА ЧЕНЯ, МЕТОД НЕОПРЕДЕЛЕННЫХ КОЭФФИЦИЕНТОВ, НОРМЕННЫЙ МЕТОД, ПОМЕХОУСТОЙЧИВОЕ КОДИРОВАНИЕ, ЗАЩИТА ИНФОРМАЦИИ.

В дипломной работе изучаются алгебраические уравнения над полями Галуа характеристики 2.

Целью дипломной работы является исследование специфики алгоритмов решения алгебраических уравнений над полями Галуа, необходимых для систем защиты информации.

Для достижения поставленной цели использовались:

- методы решения квадратных уравнений: формула и метод Ченя, метод неопределенных коэффициентов, норменный метод;
- методы решения кубических уравнений: метод Ченя, норменный метод, оптимизированный норменный метод.

В дипломной работе получены следующие результаты:

1. Описаны методы решения квадратных и кубических уравнений над полями Галуа;
2. Изученные методы реализованы в пакете Wolfram Mathematica;
3. Рассмотрен ряд примеров, иллюстрирующих специфику работы изученных методов.

Новизна результатов состоит в практической реализации норменных методов, которые ранее описывались только в теории.

Результаты дипломной работы могут быть использованы в различных приложениях алгебраических уравнений над полями Галуа.

Дипломная работа выполнена автором самостоятельно.

Thesis project is presented in the form of an explanatory note of 56 pages, 5 tables, 13 references, 5 applications.

Keyword: ALGEBRAIC EQUATIONS, GALOIS FIELDS, CHEN'S FORMULA, UNDEFINED COEFFICIENTS METHOD, NORM'S METHOD, ANTI-JAMMING CODING, INFORMATION SECURITY.

This thesis project examines algebraic equations over Galois fields of characteristic 2.

The research object is to study the specifics of algorithms for solving algebraic equations over Galois fields necessary for information security systems.

The following methods were used in the work:

- methods for solving quadratic equations: Chen's formula and Chen's method, undefined coefficients method, norm method;
- methods for solving cubic equations: Chen's method, norm's method, optimized norm's method.

The following results were obtained in the work:

1. Methods for solving square and cubic equations over Galois fields are described;
2. The methods studied are implemented in the Wolfram Mathematica package;
3. A number of examples illustrating the specifics of the work of the methods studied are considered.

The originality of the results lies in the practical implementation of norm's methods, which were previously described only in theory.

The results of the thesis can be used in various applications of algebraic equations over Galois fields.

The thesis project was done solely by the author.