

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ
Кафедра высшей алгебры и защиты информации

Аннотация к дипломной работе
АЛГОРИТМЫ РЕШЕНИЯ АЛГЕБРАИЧЕСКИХ
УРАВНЕНИЙ НАД КОНЕЧНЫМИ ПОЛЯМИ

Шатило
Александра Анатольевна

Научный руководитель:
кандидат физ.-мат. наук,
доцент
Д.В. Васильев

Минск, 2018

Дипломная работа содержит:

- 28 страниц;
- 1 рисунок;
- 10 источников;
- 1 таблица.

Ключевые слова: АЛГОРИТМЫ, АЛГОРИТМ ТОНЕЛЛИ-ШЕНКСА, АЛГОРИТМ ЧИПОЛЛЫ, СИМВОЛ ЛЕЖАНДРА, КОНЕЧНОЕ ПОЛЕ.

В дипломной работе рассматриваются алгоритмы решения алгебраических уравнений над простыми конечными полями: вероятностный алгоритм решения алгебраических уравнений произвольной степени, алгоритмы Тонелли-Шенкса и Чиполлы для решения квадратичных сравнений. Получены программные реализации алгоритмов Чиполлы и Тонелли-Шенкса при помощи библиотеки больших чисел MPIR языка программирования C++.

Главной целью работы является описание трех различных алгоритмов решения алгебраических уравнений над простым конечным полем и сравнение быстродействия двух алгоритмов решения квадратичных сравнений над конечными полями.

Дипломная работа носит практический характер. Её результаты и вывод могут быть использованы в задачах вычисления больших чисел.

Дипломная работа выполнена автором самостоятельно.

Дыпломная праца змяшчае:

- 28 старонак;
- 1 малюнак;
- 10 выкарыставаных крыніц;
- 1 табліца.

Ключавыя словы: АЛГАРЫТМЫ, АЛГАРЫТМ ТАНЭЛЛІ-ШЭНКСА, АЛГАРЫТМ ЧЫПОЛЛЫ, ЗНАК ЛЯЖАНДРА, ВЯДОМАЕ ПОЛЕ.

У дыпломнай працы разглядаюцца алгарытмы рашэння алгебраічных раўнанняў над простымі канчатковымі палямі: імавернасны алгарытм рашэння алгебраічных раўнанняў адвольнай ступені, алгарытмы Танэлі-Шенкса і Чыполлы для вырашэння квадратычным параўнанняў. Атрыманы праграмныя рэалізацыі алгарытмаў Танэлі-Шенкса і Чыполлы пры дапамозе бібліятэкі вялікіх лікаў MPFR мовы праграмавання C ++.

Галоўнай мэтай працы з'яўляецца апісанне трох розных алгарытмаў рашэння алгебраічных раўнанняў над простым канчатковым полем і параўнанне хуткадзейнасці двух алгарытмаў рашэння квадратычным параўнанняў над канчатковымі палямі.

Дыпломная праца носіць практычны характар. Яе вынікі і вывад могуць быць выкарыстаны ў задачах вылічэнні вялікіх лікаў.

Дыпломная праца выканана аўтарам самастойна.

The diploma thesis contains:

- 28 pages;
- 1 figure;
- 10 references;
- 1 table.

Key words: ALGORITHMS, TONELLI-SHENKS ALGORITHM, CIPOLLA ALGORITHM, LEJANDER SYMBOL, FINITE FIELD.

In the thesis we consider the following algorithms for solving algebraic equations over simple finite fields: probabilistic algorithm for solving algebraic equations of arbitrary degree, Tonelli-Shanks and Cipolla algorithms for solving quadratic congruences. Have been received software implementation of Cipolla and Tonelli-Shanks algorithms using the library of large numbers MPIR on C++.

The main goal of the thesis is the description of three different algorithms for solving algebraic equations over a simple finite field and a comparison of the speed of two algorithms for solving quadratic congruences over finite fields.

The diploma thesis is of practical importance. The results and inference can be used of the analysis and problems of calculating large numbers.

The thesis was written by the author independently.