БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Факультет прикладной математики и информатики

Кафедра дискретной математики и алгоритмики

Аннотация к дипломной работе

«Полиномиальные алгоритмы тестирования простоты в алгебраических числовых полях»

Прохоров Николай Петрович

Научный руководитель – кандидат физ.-мат. наук, доцент Васьковский М. М.

Минск, 2019

Реферат

Дипломная работа, 72 страницы, 5 рисунков, 1 таблица, 28 источников.

КОНЕЧНОЕ РАСШИРЕНИЕ ПОЛЯ, КОЛЬЦО ЦЕЛЫХ АЛГЕБРАИЧЕСКИХ ЭЛЕМЕНТОВ, ИДЕАЛ, ПРОСТОТА, АЛГОРИТМЫ ПРОВЕРКИ НА ПРОСТОТУ, КРИТЕРИЙ МИЛЛЕРА, КРИТЕРИЙ ЭЙЛЕРА, ТЕСТ МИЛЛЕРА-РАБИНА, АЛГОРИТМ AKS, РАСШИРЕННАЯ ГИПОТЕЗА РИМАНА, ПЛОТНОЕ МНОЖЕСТВО, ПЛОТНЫЕ КРИВЫЕ, ДИСТОРСИЯ, ТЕОРЕМА ЛЕБЕГА О ТОЧКАХ ПЛОТНОСТИ

Объект исследования – простые идеалы колец целых алгебраических элементов конечных расширений поля Q, критерии простоты идеалов и способы проверки идеалов на простоту, классы аналитических кривых комплексной плоскости, чьи образы от наклонных прямых являются плотными на комплексной плоскости.

Цель работы – получение полиномиальных детерминированных вероятностных алгоритмов проверки идеалов колец целых алгебраических элементов конечных расширений Q, построение новых классов аналитических кривых комплексной плоскости, чьи образы от наклонных прямых являются плотными на комплексной плоскости.

В ходе работы был доказан аналог критерия Миллера для идеалов колец целых алгебраических элементов конечных расширений поля Q, усиленный аналог данного критерия в случае факториальных колец целых алгебраических элементов и предположении выполнимости расширенной гипотезы Римана, вероятностный полиномиальный аналога теста Миллера-Рабина для идеалов колец целых алгебраических элементов конечных расширений поля Q, детерминированный полиномиальный аналог теста Миллера-Рабина в случае факториального кольца целых алгебраических элементов и предположении выполнимости расширенной гипотезы Римана, был построен класс аналитических кривых образ второй итерации которых от почти любой наклонной прямой плотен в C, построен класс аналитических кривых образ третьей итерации которых от любой наклонной прямой плотен в C.

Abstract

Diploma thesis, 72 pages, 5 figures, 1 tables, 28 sources.

FINITE FIELD EXTENSION, RING OF INTEGRAL ALGEBRAIC ELEMENTS, IDEAL, PRIMALITY, PRIMALITY TESTING ALGORITHMS, MILLER'S CRITERION, EULER'S CRITERION, MILLER-RABIN'S TEST, AKS ALGORITHM, EXTENDED RIEMANN HYPOTHESIS, DENSE SET, DENSE CURVE, DISTORSION, LEBESGUE'S DENSE POINT THEOREM

Object of research – prime ideals in rings of integral algebraic elements of finite extensions of field Q, primality criterion and methods to check primality of ideals, classes of analytic functions with dense on complex plane images from oblique lines.

Objective – constructing polynomial deterministic and probabilistic algorithms for primality testing of ideals in rings of integral algebraic elements of finite extensions of field Q, constructing classes of analytic functions with dense on complex plane images from oblique lines.

The results of the work are analogue of Miller's criterion for ideals in rings of integral algebraic elements of finite extensions of field Q, advanced analogue of this criterion in case when ring of integral algebraic elements is unique factorisation and under assumption that extended Riemann hypothesis holds, probabilistic polynomial analogue of Miller-Rabin`s test for ideals in rings of integral algebraic elements of finite extensions of field Q, deterministic polynomial analogue of Miller-Rabin`s test in case when ring of integral algebraic elements is unique factorisation and under assumption that extended Riemann hypothesis holds, class of analytic functions, such that image of second iteration of such functions from almost every oblique line is dense in C, class of analytic functions, such that image of third iteration of such functions from every oblique line is dense in C.