Белорусский государственный университет
Механико-математический факультет
Кафедра высшей алгберы и зашиты информации

Аннотация к дипломной работе
Субэкспоненциальные детерминированные алгоритмы тестирования на простоту

ЛАПУШИНСКИЙ
Александр Викторович

Научный руководитель:
доцент, кандидат физико-математических наук,
Д. В. Васильев

2014

Дипломная работа состоит из пяти глав, введения и заключения, общим объемом 25 с., 1 рис., 1 табл., 11 источников литературы.

Ключевые слова: ВЕРОЯТНОСТНЫЕ АЛГОРИТМЫ ТЕСТИРОВАНИЯ ПРОСТОТЫ, ДЕТЕРМИНИРОВАННЫЕ АЛГОРИТМЫ ТЕСТИРОВАНИЯ ПРОСТОТЫ, СУММЫ ЯКОБИ, ХАРАКТЕР, СУММЫ ГАУССА.

Дипломная работа «Субэкспоненциальные детерминированные алгоритмы тестирования на простоту» посвящена изучению вероятностных и детерминированных алгоритмов тестирования простоты чисел и детальному исследованию детерминированного субэкспоненциального алгоритма, созданного Х. Ленстра и Х. Коэном.

Объект исследования: Алгоритмы тестирования простоты чисел.

Цель работы: обзор детерминированных и вероятностных алгоритмов тестирования на простоту, детальное исследование алгоритма тестирования простоты чисел, созданный Х. Ленстра и Х. Коэном. Рассмотрев теоремы, на которых он базируется, получить программную реализацию и провести тестирование алгоритма.

В процессе работы выполнены следующие исследования и разработки:

1. исследованы вероятностные тесты простоты: тест Соловея-Штрассена и тест Миллера-Рабина;
2. исследованы детерминированные тесты простоты: тест AKS и тест Диемитко;
3. исследован алгоритм тестирования простоты чисел, созданный Х. Ленстра и Х. Коэном;
4. реализован алгоритм тестирования простоты чисел, созданный Х. Ленстра и Х. Коэном;
5. проведено тестирование алгоритма.

Belarusian State University
Faculty of Mechanics and Mathematics

Department of Higher Algebra and Information Security

Abstract for diploma paper

Subexponential deterministic algorithms for primality testing

Lapushinskii Aleksander Viktorovich

Supervisor

Denis Vladimirovich Vasiliev

2014

The diploma paper consists of five chapters, introduction and conclusion, total amount of 23 p., 1 fig., 1 table, 11 references .

Kee word: PROBABILISTIC ALGORITHMS FOR PRIMALITY TESTING, DETERMINISTIC ALGORITHMS FOR PRIMALITY TESTING, JACOBI SUMS, DIRICHLER CHARACTER,GAUSS SUMS.

Thesis "Subexponential deterministic algorithms for primality testing" devoted to the study of probabilistic and deterministic algorithms for primality testing, and detailed study of deterministic subexponential algorithm created Lenstroy H. and H. Cohen.

Object of research: Testing algorithms for primality.

Objective: To review detaerministic and probabilistic algorithms for testing simplicity, a detailed study of primality testing algorithm created Lenstra H. and H. Cohen, considered the theorem on which it is based, to get the software implementation and to test the algorithm.

In the diploma paper the following research and development were done:

1. Probabilistic primality tests were studied: test Solovay -Strassen and Miller-Rabin test;
2. Deterministic primality tests were studied: AKS test and test Diemitko ;
3. Algorithm for primality testing created Lenstroy H. and H. Cohen was studied;
4. Algorithm for primality testing created Lenstroy H. and H. Cohen was implemented;
5. Testing of algorithm was conducted.