МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ

Кафедра дифференциальных уравнений и системного анализа

Аннотация к дипломной работе

Методы факторизации целых чисел

Боровик Алексей Дмитриевич

Научный
руководитель:
ст преподаватель
А. В. Кушнеров

2021

В дипломной работе 38 страниц, 6 рисунков, 6 таблицы, 11 источников, одно приложение.

ФАКТОРИЗАЦИЯ ЦЕЛЫХ ЧИСЕЛ, ВЫЧИСЛИТЕЛЬНАЯ МАТЕМАТИКА, СИМВОЛ ЯКОБИ, КВАДРАТИЧНОЕ РЕШЕТО, МЕТОД ЛЕНСТРЫ, ЭЛЛИПТИЧЕСКИЕ КРИВЫЕ, ГРУППЫ, КОЛЬЦА, ПОЛЯ.

В дипломной работе изучаются методы факторизации целых чисел.

Целью дипломной работы является реализация, изученных методов факторизации, а также проведение анализа компьютерных моделей и области применения данных моделей.

Для достижения поставленной цели использовались: программный пакет Wolfram Mathematica версии 11.3, ЭВМ с параметрами: intel core i3, CPU 240 гГц, 4 гб RAM.

В дипломной работе получены следующие результаты:

1. Изучены методы факторизации целых чисел: Квадратичное решето и Метод Ленстры.
2. Реализована компьютерная модель метода квадратичного решета.
3. Реализована компьютерная модель метода Ленстры.
4. Проведено сравнение методов квадратичного решета и Ленстры.
5. Проанализирована эффективность, а также область применения на основе компьютерной модели.

Новизна работы определяется широкой применимостью ассиметричных криптосистем.

Дипломная работа имеет программно-исследовательский характер. Результаты данной работы можно применять в различных областях криптографии, таких как, ассиметричные криптосистемы.

Дипломная работа выполнена автором самостоятельно.

Thesis project is presented in the form of an explanatory note of 38 pages, 6 figures, 11 references, 1 application.

FACTORIZATION OF INTEGERS SET, COMPUTATIONAL MATHEMATICS, JACOBI SYMBOL, QUADRATIC SIEVE, LENSTRAS METHOD, ELLIPTIC CURVES, GROUPS, RINGS, FIELDS.

The research object of this thesis project is to learn working of factoring of set of integers.

The purpose of this work is to study the influence of the rate of decrease of the Fourier coefficients of the equation on the number of algebraic curves lying on the Fourier series of a dynamical system.

The purpose of this work is to make computer model of the factorization methods and analysis of this models spheres of their application area.

The following tools were used to achieve the goal: Programming package Wolfram Mathematica 11.3, computer with characteristics: intel core i3, CPU 240 gHz, 4 gb RAM.

The main results of the thesis project are as follows:

1. Methods of factorization of whole numbers: Quadratic sieve, Lenstras Method are described.
2. Computer model of quadratic sieve method are made.
3. Computer model of Lenstras method are made.
4. Comparison of two methods above and analysis of application area of computer model of these two methods are made.

The novelty of the results can be explained by application of area of asymmetric cryptosystems.

This thesis project is a research one. The results obtained in this project can be used in different areas of cryptography like asymmetric cryptosystems.

The thesis project was done solely by the author.