**МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ**

**БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ**

**МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ**

**Кафедра высшей алгебры и защиты информации**

ГРИБОВСКИЙ

Павел Олегович

**Алгоритмы проверки простоты чисел**

Аннотация к дипломной работе

Научный руководитель:

кандидат физ.-мат. наук,

 доцент С.В.Тихонов

Допущен к защите

«\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ 2023 г.

Зав. кафедрой высшей алгебры и защиты информации

доктор физ.-мат. наук, профессор В.В.Беняш-Кривец

Минск, 2023

**РЕФЕРАТ**

**Дипломная работа** содержит 37 страниц, 27 рисунков, 19 источников.

**Ключевые слова**: ПРОСТЫЕ ЧИСЛА, ЧИСЛА МЕРСЕННА, ДЕТЕРМИНИРОВАННЫЕ И ВЕРОЯТНОСТНЫЕ ТЕСТЫ ПРОСТОТЫ, АЛГОРИТМЫ, СИМВОЛЫ ЛЕЖАНДРА И ЯКОБИ, СРАВНЕНИЯ.

**Объект исследования**: простые числа.

**Цель работы**: заключается в изучении алгоритмов проверки простоты чисел, их теоретических основ, построении как можно большего простого числа, проведении анализа и сравнении полученных результатов.

Первая глава посвящена теоретико-числовым основам.

В первом параграфе рассматриваются сравнения, символы Лежандра и их свойства.

Во втором параграфе рассматриваются символы Якоби, их свойства, утверждения и теоремы, обосновывающие алгоритмы.

Вторая глава посвящена описанию некоторых детерминированных и вероятностных тестов проверки простоты чисел.

В первом параграфе рассматриваются используемые алгоритмы.

Второй параграф посвящен вычислению символов Якоби.

В третьем параграфе рассматриваются тест Соловея **–** Штрассена и время работы алгоритма.

Четвертый параграф посвящен сравнению тестов Соловея **–** Штрассена и Миллера **–** Рабина.

Пятый параграф посвящен сравнению тестов Миллера **–** Рабина и Люка **–** Лемера и нахождению максимально большого простого числа.

Третья глава посвящена программной реализации алгоритмов.

Во всех параграфах главы приводится программная реализация тестов простоты чисел на языке программирования Java.

Дипломная работа выполнена автором самостоятельно.

**ABSTRACT**

**Graduation work** consist of 37 pages, 27 illustrations, 19 references.

**Keywords**: PRIME NUMBERS, MERSENNE NUMBERS, DETERMINISTIC AND PROBABILISTIC TESTS OF PRIME NUMBERS, ALGORITHMS, LEGENDRE AND JACOBI SYMBOLS, COMPARISONS.

**Object of the researching:** prime numbers.

**Purpose of research**: is to study algorithms for testing the simplicity of numbers, their theoretical foundations, constructing as huge prime number as possible, and analyzing and comparing the results.

The first chapter is devoted to theoretical and numerical basics.

The first paragraph deals with comparisons, Legendresymbols, and their properties.

The second paragraph deals with Jacobi symbols, their properties, statements, and theorems justifying algorithms.

The second chapter is devoted to the description of some deterministic and probabilistic tests of simplicity of numbers.

The first paragraph discusses the algorithms used.

The second paragraph deals with the computation of Jacobi symbols.

The third paragraph deals with the Solovay **–** Strassen test and the running time of the algorithm.

The fourth paragraph is devoted to the comparison of the Solovay **–** Strassen and Miller **–** Rabin tests.

The fifth paragraph is devoted to comparing the Miller **–** Rabin and Lucas **–** Lehmer tests and finding the largest prime number.

The third chapter is devoted to the software implementation of the algorithms.

All paragraphs of the chapter provide a software implementation of the tests of prime numbers in the Java programming language.

The graduation project was done by the author himself.

**РЭФЕРAТ**

**Дыплoмнaя работа** змяшчае 37 старонак, 27 малюнкаў, 19 крыніц.

**Ключавыя словы**: ПРОСТЫЯ ЛІКІ, ЛІКІ МЕРСЕННА, ДЭТЭРМІНАВАНЫЯ І ІМАВЕРНАСНЫЯ ТЭСТЫ ПРАСТАТЫ, АЛГАРЫТМЫ, СІМВАЛЫ ЛЕЖАНДРА І ЯКОБІ, ПАРАЎНАННІ.

 **Aб'ект дaследaвaння**:простыя лікі.

**Цэль даследавання**: заключаецца ў вывучэнні алгарытмаў праверкі прастаты лікаў, іх тэарэтычных асноў, пабудове як мага большага простага ліку, правядзенні аналізу і параўнанні атрыманых вынікаў.

Першы раздзел прысвечаны да тэарэтыка-лікавых асноваў.

У першым параграфе разглядаюцца параўнанні, сімвалы Лежандра і іх уласцівасці.

У другім параграфе разглядаюцца сімвалы Якобі, іх уласцівасці, сцвярджэнні і тэарэмы, якія абгрунтоўваюць алгарытмы.

Другі раздзел прысвечаны апісанню некаторых дэтэрмінаваных і імавернасных тэстаў праверкі прастаты лікаў.

У першым параграфе разглядаюцца алгарытмы, якія выкары-стоўваюцца.

Другі параграф прысвечаны вылічэнням сімвалаў Якобі.

У трэцім параграфе разглядаюцца тэст Салавея **–** Штрасена і час працы алгарытму.

Чацвёрты параграф прысвечаны параўнанню тэстаў Салавея **–** Штрасена і Мілера **–** Рабіна.

Пяты параграф прысвечаны параўнанню тэстаў Мілера **–** Рабіна і Люка **–** Лемера і знаходжанню максімальна вялікага простага ліку.

Трэці раздзел прысвечаны праграмнай рэалізацыі алгарытмаў.

Ва ўсіх параграфах раздзела прыводзіцца праграмная рэалізацыя тэстаў прастаты лікаў на мове праграмавання Java.

Дыпломная праца выканана аўтарам самастойна.