МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ

Кафедра высшей алгебры и защиты информации

Коломиец Валерия Вячеславовна

Аннотация к дипломной работе:

**ДЕТЕРМИНИРОВАННЫЕ И ВЕРОЯТНОСТНЫЕ АЛГОРИТМЫ ПРОВЕРКИ ПРОСТОТЫ ЧИСЕЛ**

Научный руководитель:

кандидат физ.-мат. наук,

доцент С.В. Тихонов

Минск 2024

**АННОТАЦИЯ**

Дипломная работа состоит из 34 страниц, 5 рисунков, 5 таблиц, списка цитируемых литературных источников в количестве 9 наименований.

*Ключевые слова*: ПРОСТЫЕ ЧИСЛА, АЛГОРИТМЫ ПРОВЕРКИ ПРОСТОТЫ, ДЕТЕРМИНИРОВАННЫЕ, ВЕРОЯТНОСТНЫЕ, ТЕСТ МИЛЛЕРА-РАБИНА, ТЕСТ ФЕРМА, ТЕСТ СОЛОВЕЯ-ШТРАССЕНА, C#.

*Объектами исследования* являются детерминированные и вероятностные алгоритмы проверки простоты чисел.

*Предмет исследования* – рассмотрение теоретического описания и дальнейшая реализация детерминированных и вероятностных алгоритмов проверки простоты.

*Целью* дипломной работы является анализ точности и времени выполнения реализованных мною детерминированных и вероятностных тестов для выявления наиболее эффективного алгоритма проверки простоты.

В результате мною были исследованы детерминированные и вероятностные алгоритмы проверки простоты чисел. Были рассмотрены основные принципы работы данных алгоритмов, их преимущества и недостатки. Из детерминированных тестов я рассмотрела тест Агравала-Каяла-Саксены и тест Люка-Лемера для чисел Мерсенна. Я привела определения и теоремы, которые необходимы для понимания каждого из тестов и дальнейшего описания алгоритмов. Тест Люка-Лемера я реализовала, чтобы таким образом безошибочно получить список простых чисел Мерсенна для последующих исследований. Среди вероятностных тестов я рассматривала три наиболее известных вероятностных алгоритма: тест на основе малой теоремы Ферма, тест Соловея-Штрассена и тест Миллера-Рабина. Начала я с теоретического описания тестов и пошагового описания каждого алгоритма. Затем каждый из них я реализовала на языке программирования C# с использованием среды разработки Microsoft Visual Studio 2022, после чего сравнила точность и время выполнения.

*Практическая ценность* данной работы состоит в том, что простые числа являются основой современной криптографии, а в частности криптосистемы RSA.

*Обоснованность и достоверность* полученных результатов подтверждаются использованием проверенных алгоритмов проверки простоты, а также проведением обширного анализа реализованных тестов.

**АНАТАЦЫЯ**

Дыпломная праца складаецца з 34 старонак, 5 малюнкаў, 5 табліц, спісу цытуемых літаратурных крыніц у колькасці 9 найменняў.

*Ключавыя словы*: ПРОСТЫЯ ЛІКІ, АЛГАРЫТМЫ ПРАВЕРКІ ПРАСТАТЫ, ДЭТЭРМІНАВАНЫЯ, ІМАВЕРНАСНЫЯ, ТЭСТ МІЛЕРА-РАБІНА, ТЭСТ ФЕРМА, ТЭСТ САЛАВЕЯ-ШТРАСЭНА, C#.

*Аб'ектамі даследавання* з'яўляюцца дэтэрмінаваныя і імавернасныя алгарытмы праверкі прастаты лікаў.

*Прадмет даследавання -* разгляд тэарэтычнага апісання і далейшая рэалізацыя дэтэрмінаваных і імавернасных алгарытмаў праверкі прастаты*.*

*Мэтай* дыпломнай працы з'яўляецца аналіз дакладнасці і часу выканання рэалізаваных мною дэтэрмінаваных і імавернасных тэстаў для выяўлення найбольш эфектыўнага алгарытму праверкі прастаты.

У выніку мною былі даследаваны дэтэрмінаваныя і імавернасныя алгарытмы праверкі прастаты лікаў. Былі разгледжаны асноўныя прынцыпы працы дадзеных алгарытмаў, іх перавагі і недахопы. З дэтэрмінаваных тэстаў я разгледзела тэст Агравала-Каяла-Саксэны і тэст Люка-Лямера для лікаў Мярсэна. Я прывяла вызначэння і тэарэмы, якія з'яўляюцца неабходнымі для разумення кожнага з тэстаў і далейшага апісання алгарытмаў. Тэст Люка-Лямера я рэалізавала, каб такім чынам беспамылкова атрымаць спіс простых лікаў Мярсена для наступных даследаванняў. Сярод імавернасных тэстаў я разглядала тры найбольш вядомых імавернасных алгарытма: тэст на аснове малой тэарэмы Ферма, тэст Салавея-Штрасэна і тэст Мілера-Рабіна. Пачала я з тэарэтычнага апісання тэстаў і пакрокавага апісання кожнага алгарытму. Затым кожны з іх я рэалізавала на мове праграмавання C # з выкарыстаннем асяроддзя распрацоўкі Microsoft Visual Studio 2022, пасля чаго параўнала дакладнасць і час выканання.

*Практычная каштоўнасць* дадзенай працы складаецца ў тым, што простыя лікі з'яўляюцца асновай сучаснай крыптаграфіі, а калі дакладней крыптасістэмы RSA*.*

*Абгрунтаванасць і дакладнасць* атрыманых вынікаў пацвярджаюцца выкарыстаннем правераных алгарытмаў праверкі прастаты, а таксама правядзеннем шырокага аналізу рэалізаваных тэстаў.

**ANNOTATION**

The thesis consists of 34 pages, 5 figures, 5 tables, a list of cited literary sources in the amount of 9 titles.

*Key words*: PRIME NUMBERS, ALGORITHMS FOR CHECKING SIMPLICITY, DETERMINISTIC, PROBABILISTIC, MILLER-RABIN TEST, FERMAT TEST, SOLOVAY-STRASSEN TEST, C#.

*The objects of research* are deterministic and probabilistic algorithms for checking the simplicity of numbers.

*The subject of the study* is the consideration of the theoretical description and further implementation of deterministic and probabilistic algorithms for checking simplicity.

*The purpose* of the thesis is to analyze the accuracy and execution time of the deterministic and probabilistic tests I have implemented in order to identify the most effective algorithm for checking simplicity.

As a result, I have investigated deterministic and probabilistic algorithms for checking the simplicity of numbers. The basic principles of operation of these algorithms, their advantages and disadvantages were considered. Of the deterministic tests, I considered the Agrawal-Kayal-Saxena test and the Lucas-Lehmer test for Mersenne numbers. I have given definitions and theorems that are necessary to understand each of the tests and further describe the algorithms. I implemented the Lucas-Lehmer test in order to accurately obtain a list of Mersenne primes for subsequent research. Among the probabilistic tests, I considered three of the most famous probabilistic algorithms: the test based on Fermat's small theorem, the Solovay-Strassen test and the Miller-Rabin test. I started with a theoretical description of the tests and a step-by-step description of each algorithm. Then I implemented each of them in the C# programming language using the Microsoft Visual Studio 2022 development environment, after which I compared the accuracy and execution time.

*The practical value* of this work lies in the fact that prime numbers are the basis of modern cryptography, and in particular the RSA cryptosystem.

*The validity and reliability* of the results obtained are confirmed by the use of proven simplicity verification algorithms, as well as by conducting an extensive analysis of the implemented tests.