МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
МЕХАНИКО_МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ

Кафедра высшей алгебры и защиты информации

Филонец Полина Юрьевна

$(N \pm 1)$ – методы проверки простоты чисел

Дипломная работа

Научный руководитель:
кандидат физ.-мат. наук, доцент
Тихонов Сергей Викторович

Допущена к защите
«__»_____2017 г.
_____
Зав. кафедрой высшей алгебры
и защиты информации,
доктор физ.-мат. наук, профессор
Беняш-Кривец Валерий Вацлавович

Минск 2017

Аннотация

Дипломная работа содержит 37 страниц и 9 литературных источника.

Ключевые слова: ПРОСТЫЕ ЧИСЛА, КЛАССЫ ВЫЧЕТОВ, МУЛЬТИПЛИКАТИВНАЯ ГРУППА КОЛЬЦА, ПОРЯДОК ЭЛЕМЕНТА, СИМВОЛ ЛЕЖАНДРА, ($N \pm 1$) – МЕТОДЫ ПРОВЕРКИ ПРОСТЫХ ЧИСЕЛ, АЛГОРИТМЫ ПОСТРОЕНИЯ БОЛЬШИХ ПРОСТЫХ ЧИСЕЛ.

Цель работы заключается в изучении ($N \pm 1$) – методов проверки простоты чисел, а также некоторых способах построения больших простых чисел, широко используемых в криптографии.

Первая глава посвящена изучению основных определений и теорем, которые используются при доказательстве теорем связанных с проверкой чисел на простоту.

Вторая глава посвящена ($N \pm 1$) – методам проверки простоты чисел.

В первом параграфе рассматриваются (N-1) – методы проверки простоты чисел.

Во втором параграфе рассматриваются (N+1) – методы проверки простоты чисел.

В третьем параграфе рассматриваются некоторые способы построения больших простых чисел, широко используемых в криптографии.

Анатацыя

Дыпломны праект змяшчае 37 старонак і 9 літаратурных крыніц. **Ключавыя словы:** ПРОСТЫЯ ЛІКІ, КЛАССЫ РЭШТАЎ, МУЛЬТЫПЛІКАТЫЎНАЯ ГРУППА КОЛЦА, ПАРАДАК ЭЛЕМЕНТА, СІМВАЛ ЛЕЖАНДРА, ($N \pm 1$) – МЕТАДЫ ПРАВЕРКІ ПРОСТАТЫ ЛІКАЎ, АЛГАРЫТМЫ ПАБУДОВЫ ВЯЛІКІХ ПРОСТЫХ ЛІКАЎ.

Мэта работы заключаецца ў вывучэнні ($N \pm 1$) – метадаў праверкі прастаты лікаў, а таксама некаторых спосабах пабудовы вялікіх простых лікаў, якія шырока выкарыстоўваюцца ў крыптаграфіі.

Першая частка прысвечана вывучэнню асноўных азначэнняў і тэарэм, якія выкарыстоўваюцца пры доказе тэарэм, звязаных з праверкай лікаў на прастату.

Другая часткапрысвечана ($N \pm 1$) – метадам праверкі прастаты лікаў.

У першым параграфе разглядаюцца (N-1) – метады праверкі прастаты лікаў.

У другім параграфе разглядаюцца (N + 1) – метады праверкі прастаты лікаў.

У трэцім параграфе разглядаюцца некаторыя спосабы пабудовы вялікіх простых лікаў, якія шырока выкарыстоўваюцца ў крыптаграфіі.

Abstract

The thesis contains 37 pages and 9 references.

Keywords: PRIME NUMBERS, RESIDUE CLASSES, THE MULTIPLICATIVE GROUP OF THE RING, THE ORDER OF THE ELEMENT, THE LEGENDRE SYMBOL, ($N \pm 1$)-METHODS FOR CHECKING PRIME NUMBERS, ALGORITHMS CONSTRUCTING LARGE PRIME NUMBERS.

The purpose of work is to study ($N \pm 1$) – methods for testing the simplicity of numbers, as well as some ways of constructing large prime numbers widely use dincryptography.

The first chapter is devoted to the study of the main definitions and theorems used in the proof of theorems related to the verification of numbers for simplicity.

The second chapter is devoted to ($N \pm 1$) – methods for verifying the simplicity of numbers.

In the first section we consider (N-1) – methods for testing the simplicity of numbers.

In the second section we consider ($N \pm 1$) – methods for testing the simplicity of numbers.

In the third section, some methods for constructing large prime numbers widely used in cryptography are considered.