МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ

Кафедра высшей алгебры и защиты информации

Дипломная работа

ПЕРВООБРАЗНЫЕ КОРНИ И ИХ ПРИЛОЖЕНИЯ

СТАСЕЛЬКО Павел Владимирович

Научный руководитель:
кандидат физико-
математических наук, доцент
_____ Тихонов С.В.

Допущен к защите
«____» _____2021 г.

Заведующий кафедрой алгебры и
защиты информации
профессор, доктор физ.-мат. наук
_____ В. В. Беняш-Кривец

Минск, 2021

РЕФЕРАТ

Дипломная работа содержит 34 с., 13 рис., 6 источников.

Ключевые слова: *первообразные корни, алгоритм нахождения первообразного корня, индекс числа, алгоритм нахождения индекса числа, приложения первообразных корней.*

Цель работы заключается в изучении свойств первообразных корней, их приложений, а также программной реализации алгоритмов поиска первообразных корней и индексов.

Первая глава посвящена теоретико-числовым основам.

В первом параграфе рассматриваются основные понятия теории сравнений.

Во втором параграфе рассматриваются общие теоремы теории сравнений.

В третьем параграфе изучаются первообразные корни по модулям p^α и $2p^\alpha$.

В четвертом параграфе рассматриваются методы нахождения первообразных корней по модулям p^α и $2p^\alpha$.

Вторая глава посвящена программной реализации нахождения первообразных корней.

В первом параграфе рассматриваются вспомогательные алгоритмы, необходимые для решения основной задачи.

Во втором параграфе приводится алгоритм нахождения первообразного корня.

Третья глава посвящена приложениям первообразных корней.

В первом параграфе рассматриваются индексы и двучленные сравнения.

Во втором параграфе приводится алгоритм поиска индекса числа по некоторому модулю.

РЭФЕРАТ

Дыпломны праект змяшчае 34 с., 13 мал., 6 крыніц.

Ключавыя словы: *першаісныя карані, алгарытм знаходжання першаіснага кораня, індэкс колькасці, алгарытм знаходжання індэкса колькасці, прыкладання першаіснных каранёў*.

Мэта работы заключаецца ў вывучэнні ўласцівасцяў першаісных каранёў, іх прыкладанняў, а таксама праграмнай рэалізацыі алгарытмаў пошуку першаісных каранёў і індэксаў.

Першая глава прысведчана тэарэтыка-лічбавым асновам.

У першым параграфе разглядаюцца асноўныя паняцці тэорыі параўнанняў.

У другім параграфе разглядаюцца агульныя тэарэмы тэорыі параўнанняў.

У трэцім параграфе вывучаюцца першаісныя карані па модулях p^α і $2p^\alpha$.

У чацвёртым параграфе разглядаюцца метады знаходжання першаісных каранёў па модулях p^α і $2p^\alpha$.

Другая частка прысведчана праграмнай рэалізацыі знаходжання першаісных каранёў.

У першым параграфе разглядаюцца дапаможныя алгарытмы, неабходныя для вырашэння асноўнай задачы.

У другім параграфе прыводзіцца алгарытм знаходжання першаіснага кораня.

Трэцяя частка прысведчана прыкладанням першаісных каранёў.

У першым параграфе разглядаюцца індэксы і двучленныя параўнання.

У другім параграфе прыводзіцца алгарытм пошуку індэкса колькасці па некаторым модулю.

ABSTRACT

The thesis contains 34 p., Figures 13, 6 sources.

Key words: *primitive roots, an algorithm for finding an primitive root, index of a number, an algorithm for finding an index of a number, application of primitive roots.*

The purpose of the work is to study the properties of primitive roots, their applications, as well as the software implementation of algorithms for finding primitive roots and indices.

The first chapter is devoted to number theory foundations.

The first section discusses the basic concepts of the theory of comparisons.

In the second section, general theorems of the theory of comparisons are considered.

In the third section, we study the antiderivative roots modulo p^{α} and $2p^{\alpha}$.

In the fourth section, we consider methods for finding primitive roots modulo p^{α} and $2p^{\alpha}$.

The second chapter is devoted to the software implementation of finding primitive roots.

In the first section, we consider auxiliary algorithms needed to solve the main problem.

In the second section, an algorithm for finding the primitive root is given.

The third chapter is devoted to applications of primitive roots.

The first section deals with indices and binomial comparisons.

In the second section, an algorithm for finding the index of a number by some modulus is given.