МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ
Кафедра высшей алгебры и защиты информации

Жук
Павел Витальевич

ЭЛЛИПТИЧЕСКИЕ КРИВЫЕ НАД КОНЕЧНЫМИ ПОЛЯМИ

Дипломная работа

Научный руководитель:
доцент кафедры высшей алгебры
и защиты информации
кандидат физ.-мат. наук
Тихонов Сергей Викторович

Допущена к защите

«___» _____ 2021 г.

Зав. кафедрой высшей алгебры и защиты информации

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

Минск, 2021

Реферат

Работа состоит из 39 страниц, при написании использовано 6 источников, содержит 3 таблицы, 11 рисунков, большое количество математических формул, определений и теорем.

В дипломной работе рассматриваются эллиптические кривые, в частности, над конечными полями, и их свойства.

При исследовании и написании использовались материалы научных статей и публикаций из различных журналов, в том числе и зарубежных.

В первой главе рассматриваются определения группы, кольца, поля и их свойства.

Во второй главе рассматриваются определение и свойства эллиптических кривых, групповой закон точек эллиптической кривой.

В третьей главе приведены примеры вычислений порядка группы точек эллиптических кривых над конечными полями.

Рэферат

Праца складаецца з 39 старонак, пры напісанні выкарыстана 6 крыніц, змяшчае 3 табліцы, 11 малюнкаў, вялікую колькасць матэматычных формул, азначэнняў і тэарэм.

У дыпломнай працы разглядаюцца эліптычныя крывыя, у прыватнасці, над канчатковымі палямі, і іх ўласцівасці.

Пры даследаванні і напісанні выкарыстоўваліся матэрыялы навуковых артыкулаў і публікацый з розных часопісаў, у тым ліку і замежных.

У першай чале разглядаюцца вызначэння групы, кольцы, палі і іх ўласцівасці.

У другой чале разглядаюцца вызначэнне і ўласцівасці эліптычных крывых, Групавы закон пунктаў эліптычнай крывой.

У трэцяй чале прыведзены прыклады вылічэнняў парадку групы пунктаў эліптычных крывых над канчатковымі палямі.

Abstract

The work consists of 39 pages, 6 sources were used in writing, it contains 3 tables, 11 figures, a large number of mathematical formulas, definitions and theorems.

The thesis deals with elliptic curves, in particular, over finite fields, and their properties.

Materials of scientific articles and publications from various journals, including foreign ones, were used in the research and writing.

The first chapter discusses the definitions of groups, rings, fields, and their properties.

The second chapter deals with the definition and properties of elliptic curves, the group law of points of an elliptic curve.

The third chapter provides examples of computing the order of a group of points of elliptic curves over finite fields.