МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ

Кафедра высшей алгебры и защиты информации

Дипломная работа

ФАКТОРИЗАЦИЯ ЦЕЛЫХ ЧИСЕЛ С ПОМОЩЬЮ ЭЛЛИПТИЧЕСКИХ КРИВЫХ

ЛУТОВ Глеб Андреевич

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

Допущен к защите
«____» _____2020 г.

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

Минск, 2020

РЕФЕРАТ

Дипломная работа содержит 36 с., 1 рис., 19 источников.

Ключевые слова: *натуральные числа, факторизация числа, эллиптические кривые, метод Ленстры факторизации с помощью эллиптических кривых.*

Цель работы заключается в изучении метода Ленстры факторизации целых чисел с помощью эллиптических кривых и его программной реализации.

Первая глава посвящена к теоретико-числовым основам.

В первом параграфе рассматривается факторизация целых чисел.

Во втором параграфе рассматриваются различные методы факторизации.

В третьем параграфе рассматриваются эллиптические кривые.

В четвертом параграфе рассматриваются канонические формы уравнений эллиптической кривой.

В пятом параграфе рассматривается групповой закон эллиптических кривых.

Вторая глава посвящена факторизации при помощи эллиптических кривых.

В первом параграфе рассматриваются необходимые для этого определения.

Во втором параграфе рассматривается метод Ленстры факторизации с помощью эллиптических кривых.

Третья глава посвящена программной реализации метода Ленстры факторизации с помощью эллиптических кривых.

В первом параграфе рассматривается программная реализация, основанная на примере из второго параграфа второй главы, получающая разложение числа.

Во втором параграфе рассматривается программная реализация нахождения множителей, зная уже один.

В третьем параграфе производится анализ метода Ленстры.

РЭФЕРАТ

Дыпломны праект змяшчае 36 с., 1 мал., 19 крыніц.

Ключавыя словы: *натуральныя лікі, фактарызацыя колькасці, эліптычныя крывыя, метад Ленстры фактарызацыі з дапамогай эліптычных крывых.*

Мэта работы заключаецца у вывучэнні метада Ленстры фактарызацыі з дапамогай эліптычных крывых і яго праграмнай рэалізацыі.

Першая глава прысведчана тэарэтыка-лічбавым асновам.

У першым параграфе разглядаецца фактарызацыя цэлых лікаў.

У другім параграфе разглядаюцца розныя метады фактарызацыі.

У трэйцім параграфе разглядаюцца эліптычныя крывыя.

У чацвёртым параграфе разлядаюцца кананічныя формы раўнанняў эліптычнай крывой.

У пятым параграфе разглядаецца групавы закон эліптычных крывых.

Другая глава прысведчана фактарызацыі пры дапамозе эліптычных крывых.

У першым параграфе разглядаюцца неабходныя для гэтага вызначэння.

У другім параграфе разглядаецца метад Ленстры фактарызацыі з дапамогай эліптычных крывых.

Трэцяя глава прысведчана праграмнай рэалізацыі метаду Ленстры фактарызацыі з дапамогай эліптычных крывых.

У першым параграфе разглядаецца праграмная рэалізацыя заснаваная на прыкладзе з другога параграфа другой часткі, якая атрымоўвае разлажэнне лічбы.

У другім параграфе разглядаецца праграмная рэалізацыя знаходжання множнікаў, ведаючы ўжо адзін.

У трэцім параграфе вырабляецца аналіз метаду Ленстры.

ABSTRACT

The thesis contains 36 p., Figures 1, 19 sources.

Keywords: *natural numbers, integer factorization, elliptic curves, Lenstra elliptic curve factorization method.*

The purpose of the work is to study the Lenstra elliptic curve factorization method and its software implementation.

The first chapter is devoted to theoretical and numerical basics.

In the first section we consider integer factorization.

In the second section we consider various factorization methods.

In the third section we consider elliptic curves.

In the fourth section we consider the canonical forms of elliptic curve equations.

In the fifth section we consider the group law of elliptic curves.

The second chapter is devoted to factorization using elliptic curves.

In the first section we consider the necessary definitions.

In the second section we consider the Lenstra elliptic curve factorization method.

In the third section we consider another algorithms for calculating of Jacobi symbol.

The third chapter is devoted to software implementation of the Lenstra elliptic curve factorization method.

In the first section we consider software implementation based on the example from the second paragraph of the second chapter that receives a decomposition of a number.

In the second section we consider software implementation of finding the factors, knowing one already.

In the third section we consider analysis of the Lenstra method.