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

Аннотация к дипломной работе

ПРИВЕДЕННЫЕ БАЗИСЫ РЕШЕТОК И ФАКТОРИЗАЦИЯ МНОГОЧЛЕНОВ

ЛУКАШЕВИЧ Александр Викторович

Научный руководитель:

профессор Беняш-Кривец Валерий Вацлавович

Минск, 2015

РЕФЕРАТ

Дипломная работа содержит:

- 105 страниц
- 4 приложения
- 5 использованных источников

Ключевые слова: МНОГОЧЛЕН, ФАКТОРИЗАЦИЯ МНОГОЧЛЕНА, LLL-АЛГОРИТМ, СЛОЖНОСТЬ АЛГОРИТМА, ПОДЪЕМ ГЕНЗЕЛЯ.

В дипломной работе изучаются алгоритмы факторизации многочленов над полем рациональных чисел.

Целью данной дипломной работы является сравнение классического и практического вариантов реализации LLL-алгоритма факторизации многочленов над полем рациональных чисел, выявление причин популярности использования более медленного в оценке практического алгоритма.

Для достижения поставленной цели использовались материалы отечественных и зарубежных авторов с описанием вышеупомянутых алгоритмов, а также математический пакет «WolframMathematica».

В дипломной работе получены следующие результаты:

- обоснована корректность работы исследуемых алгоритмов
- выявлены шаги алгоритмов, на которых практический алгоритм факторизует конкретные многочлены быстрее
- предложены пути усовершенствования алгоритмов

Новизна работы состоит в параллельном сравнении реализации алгоритмов на конкретных примерах.

Дипломная работа носит как теоретический так и практический характер. Ее данные могут быть использованы студентами нашего университета для более глубокого изучения темы факторизации многочленов.

Дипломная работа выполнена автором самостоятельно.

РЭФЕРАТ

Дыпломная работазмяшчае:

- 105 старонак
- 4 прыкладання
- 5 выкарыстаныхкрыніц

Ключавыясловы: МНАГАСКЛАДНІК, ФАКТАРЫЗАЦЫЯ МНАГАСКЛАДНІКА, LLL-АЛГАРЫТМ, СКЛАДАНАСЦЬ АЛГАРЫТМАЎ, УЗДЫМ ГЕНЗЭЛЯ.

У дыпломнайрабоцевывучаюццаалгарытмыфактарызацыімнагаскладніка над полем рацыянальныхлікаў.

Мэтайдадзенайдыпломнай работыз'яўляецццапараўнаннекласічнага і практычнагаварыянтаўрэалізацыі LLL-алгарытмуфакторызацыімнагачлена над полем рацыянальныхлікаў, выяўленнепрычынпапулярнасцівыкарыстаннябольшпавольнага ў ацэнцыпрактычнагаалгарытму.

Для дасягненняпастаўленаймэтывыкарыстоўвалісяматэрыялыайчынных і замежныхаўтараў з апісаннемвышэйзгаданыхалгарытмаў, а таксамаматэматычны пакет «WolframMathematica».

У дыпломнайрабоцеатрыманынаступныявынікі:

- абгрунтаванакарэктнасцьпрацыдоследныхалгарытмаў
- выяўленыкрокіалгарытмаў, наякіхпрактычныалгарытмфактарызуе канкрэтныямнагаскладнікіхутчэй
- прапанаванышляхіўдасканаленняалгарытмаў

Навізна работыскладаецца ў паралельнымпараўнаннірэалізацыіалгарытмаў на канкрэтныхпрыкладах.

Дыпломная работаносіць як тэарэтычны так і практычныхарактар. Яедадзеныямогуцьбыцьвыкарыстаныстудэнтамінашагаўніверсітэта для большглыбокагавывучэннятэмы фактарызацыімнагачленаў.

Дыпломнаяработавыкананаўтарамсамастойна.

ABSTRACT

This diploma thesis contains:

- 105 pages
- 4 applications
- 5 sources used

Keywords: POLYNOMIAL, FACTORING A POLYNOMIAL, LLL-ALGORITHM, COMPLEXITY OF ALGORITHMS, LIFTING HANSEL.

The research paper examines algorithms factoring polynomials over a field of rational numbers.

The aim of this thesis is the comparison of classical and practical embodiments of the LLL-algorithm for factoring polynomials over a field of rational numbers, identifying reasons for the popularity of using slower in evaluating the practical algorithm.

To achieve this goal the materials used domestic and foreign authors with a description of the above algorithms and mathematical package «Wolfram Mathematica».

In the research paper the following results:

- proved the correctness of the test algorithms
- identified the steps of algorithms in which practical algorithm factors the specific polynomials faster
- suggest ways to improve algorithms

The novelty of the work lies in the parallel implementation of algorithms compared with concrete examples.

Diploma work is both theoretical and practical. Its data can be used by students of the University for a deeper study of the topic factoring polynomials.

Thesis work is done by the author alone.