

АЛГЕБРАИЧЕСКИЙ ПРОЦЕССОР ДЛЯ ДИСТАНЦИОННОГО ОБУЧЕНИЯ КОМПЬЮТЕРНОЙ АЛГЕБРЕ И КРИПТОГРАФИИ

ТИП ПРЕДЛАГАЕМОЙ ПРОДУКЦИИ/УСЛУГИ

- программный продукт
- услуги
 - образовательные услуги, в том числе по переподготовке специалистов

ОБЛАСТЬ ЗНАНИЙ

27	Математика
27.17	Алгебра
27.17.27	Поля и многочлены
50	Автоматика и вычислительная техника
50.41	Программное обеспечение вычислительных машин, комплексов и сетей
50.41.25	Прикладное программное обеспечение

ОБЛАСТИ ПРИМЕНЕНИЯ

1. Образование.
2. Научные исследования.

ПРИМЕРЫ ПРИМЕНЕНИЯ

Используется в учебном процессе кафедры Математического моделирования по дисциплинам «Дискретная математика», «Современная компьютерная алгебра» и «Методы защиты информации и распознавания образов» (рис. 1-3).

Алгебраический процессор



Кафедра
Математического Моделирования

Дистанционный электронный образовательный ресурс АЛГЕБРАИЧЕСКИЙ ПРОЦЕССОР «НИУ «МЭИ» поддерживает теоретическое и практическое изучение свойств и алгоритмов

Дистанционный электронный АЛГЕБРАИЧЕСКИЙ ПРОЦЕССОР получил финансовую поддержку РФФ локальной версии, разработана программа Инновационные математического моделирования университета «МЭИ».

Программное обеспечение
Свидетельство о государственной регистрации 2012617762 MPEI Processor - алгебраических операций из алгебраической библиотеки

Рис. 1. Фрагмент титульной страницы алгебраического процессора

Практикум

Лабораторная работа №1. Вычисления в числовых алгебраических структурах

Теоретическое
введение

Лабораторная работа №3. Алгоритм согласования для дискретного логарифмирования

Рис. 2. Фрагмент рабочего стола алгебраического процессора со ссылками на две лабораторные работы

Лекции СКА гр. А-14-14

А-14-14 (СКА)
Календарный план и литература
Лекция 1. Вычисления в Числовых алгебраических структурах
Лекция 2. Квадратичные вычеты. Символы Лежандра и Якоби. Проблема квадратичного вычета. Числа Блюма
Лекция 3. Квадратные корни из квадратичных вычетов. Проблема квадратного корня
Лекция 4. Криптосистемы с открытым ключом: Рабина, Гольдвассер - Миколи, Блюма-Гольдвассер
Лекция 5. Тесты разложимости и тесты простоты. порождение больших простых чисел
Лекция 6. Характеристика и мультипликативная группа поля. Многочлены над полем. Простое, алгебраическое и конечное расширения поля и операции в них.
Лекция 7. Неприводимые многочлены. тестирование и поиск неприводимых многочленов.
Лекция 8. Методы ускорения вычислений. Монтгомери, Китайская теорема об остатках.
Лекция 9 (дополнение). Метод Карацубы. Метод Штраусена.
Лекция 9. Линейные рекуррентные последовательности.

Укажите количество по методу Карацубы-Лаб.
работа к лекции 8 в А-14-14

Рис. 3. Фрагмент рабочего стола Алгебраического процессора по дисциплине Современная компьютерная алгебра с обращением к лабораторной работе по методу Карацубы.

КРАТКОЕ ОПИСАНИЕ

- Дистанционный электронный образовательный ресурс АЛГЕБРАИЧЕСКИЙ ПРОЦЕССОР «НИУ «МЭИ» поддерживает теоретическое и практическое изучение свойств и алгоритмов конечных групп, колец, полей и основанных на этих алгебраических структурах средств защиты информации, в частности, криптографических систем и протоколов.
- Отличается широким набором изучаемых алгебраических структур и позволяет выполнять вычисления в них с использованием составляемых в интерактивном режиме программ на основе библиотеки классов MPEI AAL (MPEI Algebraic Abstractions Library).
- Предназначен для использования при выполнении лабораторных работ, курсовых и дипломных проектов, выпускных работ бакалавров и других видов самостоятельной работы, а также для демонстрации изучаемых алгебраических аспектов дисциплины при чтении лекций.

ОСОБЕННОСТИ

Использование в режиме дистанционного доступа, как для теоретического обучения, так и для выполнения расчетов и компьютерных экспериментов с доступом к алгебраическим библиотекам.

ПРАВОВАЯ ЗАЩИТА

1. Свидетельство о государственной регистрации программы для ЭВМ. № 2013618585. Полиномиальный класс алгебраической библиотеки AAL MPEI.
2. Свидетельство о государственной регистрации программы для ЭВМ. № 2013615738. Дистанционный информационный ресурс вычислений с использованием алгебраических библиотек.
3. Свидетельство о государственной регистрации программы для ЭВМ № 2012617762. MPEI Processor - программа интерактивного исполнения алгебраических операций различных алгебраических структур на основе алгебраической библиотеки MPEI ALL.

КОНТАКТЫ

Разработчик: Фролов Александр Борисович,

Институт автоматизации и вычислительной техники, каф. Математического моделирования