

КОМПЬЮТЕРНАЯ АЛГЕБРА

1. Цель освоения дисциплины

Формирование универсальных и профессиональных компетенций у обучающихся, готовности к использованию систематизированных знаний в области абстрактной и компьютерной алгебры при решении задач профессиональной деятельности учителя математики.

2. Место дисциплины в структуре ОПОП

Дисциплина «Компьютерная алгебра» относится к вариативной части блока дисциплин. Для освоения дисциплины «Компьютерная алгебра» обучающиеся используют знания, умения, способы деятельности и установки, сформированные в ходе изучения дисциплин «Алгебра», «Геометрия», «Дискретная математика», «Дифференциальные уравнения», «Информационные системы», «Математическая логика и теория алгоритмов», «Математический анализ», «Методика обучения математике», «Практикум по решению предметных задач», «Программирование», «Программное обеспечение систем и сетей», «Теоретические основы информатики», «Теория вероятностей и математическая статистика», «Теория функций действительного переменного», «Теория чисел», «Числовые системы», «Элементарная математика», «3D-моделирование и печать», «Вводный курс математики», «Компьютерные сети», «Образовательная робототехника», «Практикум решения школьных математических задач», прохождения практик «Учебная (ознакомительная по информатике) практика», «Учебная (ознакомительная по математике) практика», «Учебная (ознакомительная по элементарной математике) практика». Освоение данной дисциплины является необходимой основой для последующего изучения дисциплин «Архитектура компьютера», «Веб-технологии», «Информационная безопасность и защита информации», «Теория игр и исследование операций», «Методика использования интерактивных средств при обучении математике», «Перспективные направления искусственного интеллекта», «Перспективные направления компьютерного моделирования», «Цифровая дидактика математического образования».

3. Планируемые результаты обучения

В результате освоения дисциплины выпускник должен обладать следующими компетенциями:

– способен осваивать и использовать теоретические знания и практические умения и навыки в предметной области при решении профессиональных задач (ПК-1).

В результате изучения дисциплины обучающийся должен:

знать

- способы представления на компьютере классических алгебраических структур, границы применимости символьных вычислений на компьютере;
- основные методы и алгоритмы компьютерной алгебры;
- базовые методы перечисления конечных алгебраических объектов;
- строение конечных полей;
- свойства конечных полей, позволяющие осуществить эффективную факторизацию полиномов над ними;

уметь

- решать с использованием математических пакетов базовые задачи, относящиеся к компьютерной алгебре;
- применять основные алгоритмы, реализованные в системе компьютерной алгебры, для

решения задач теории чисел;

- решать типовые задачи на разбиение множества равномоощных конечных алгебраических объектов с одинаковой сигнатурой на классы изоморфных;
- представлять конечные поля на компьютере;
- реализовывать алгоритм Берлекэмпа;

владеть

- представлением о связи абстрактной алгебры и символьных вычислений на компьютере;
- приемами использования системы компьютерной алгебры для решения задач теории чисел;
- приемами реализации базовых алгоритмов на графах;
- методами вычислений в конечных полях на компьютере;
- приемами оценки вычислительной сложности задач факторизации полинома над тем или иным конечным полем.

4. Общая трудоёмкость дисциплины и её распределение

количество зачётных единиц – 3,

общая трудоёмкость дисциплины в часах – 108 ч. (в т.ч. аудиторных часов – 32 ч., СРС – 72 ч.),

распределение по семестрам – 9,

форма и место отчётности – аттестация с оценкой (9 семестр).

5. Краткое содержание дисциплины

Символьные вычисления на компьютере.

Символьные вычисления на компьютере. Предмет компьютерной алгебры. Проблемы разбухания данных. Алгоритмическая неразрешимость проблемы тождества слов в основных алгебраических структурах и ее влияние на развитие компьютерной алгебры. Основные формы и представления алгебраических объектов и выражений на компьютере.

Арифметика целых чисел на компьютере.

Сравнение, сложение, вычитание и умножение целых чисел в компьютерной алгебре.

Деление с остатком. Возведение в степень по модулю, числа Кармайкла. Бинарный алгоритм и алгоритм Евклида. Сильный тест проверки на псевдопростоту Рабина-Миллера.

Детерминированные тесты. Простые числа Мерсенна. Тест Люка-Лемера и проект GIMPS.

Классические и современные алгоритмы факторизации натуральных чисел: метод Ферма; метод Моррисона-Бриллхарта; метод квадратичного решета. Проблема надежности RSA-шифрования с открытым ключом.

Работа с конечными алгебраическими структурами.

Особенности работы с конечными алгебраическими структурами на компьютере. Работа с группами подстановок: перевод подстановки, заданной второй строкой двухстрочной записи, в цикловую форму, и обратное построение подгруппы группы подстановок с заданным множеством образующих. Алгоритмы на графах. Перечисление всех квазигрупп (луп) фиксированного порядка с точностью до изоморфизма. Проверка выполнимости тождеств и квазитожеств в конечных алгебраических структурах.

Конечные поля.

Существование простого подполя. Теорема существования и единственности для конечных полей. Структура подполей конечного поля. Строение мультипликативной группы конечного поля. Конечное поле как простое алгебраическое расширение простого конечного поля.

Представление конечных полей на компьютере. Конечное поле как множество всех корней всех неприводимых над любым подполем полиномов, степени которых делят степень расширения исходного поля над данным подполем.

Факторизация многочленов над конечными полями.

Отделение кратных корней многочленов над конечными полями. Теоретические основы алгоритма Берлекэмпса. Реализация алгоритма Берлекэмпса. Случай полей большой характеристики.

6. Разработчик

Лецко Владимир Александрович, кандидат педагогических наук, доцент кафедры высшей математики и физики ФГБОУ ВО «ВГСПУ»,

Астахова Наталья Александровна, кандидат педагогических наук, доцент кафедры высшей математики и физики ФГБОУ ВО «ВГСПУ».