

# КОМПЬЮТЕРНАЯ АЛГЕБРА

## 1. Цель освоения дисциплины

Формирование систематизированных знаний в области компьютерной алгебры.

## 2. Место дисциплины в структуре ОПОП

Дисциплина «Компьютерная алгебра» относится к вариативной части блока дисциплин и является дисциплиной по выбору.

Для освоения дисциплины «Компьютерная алгебра» обучающиеся используют знания, умения, способы деятельности и установки, сформированные в ходе изучения дисциплин «Естественнонаучная картина мира», «Информационные технологии в образовании», «Основы математической обработки информации», «Педагогика», «Психология», «Абстрактная и компьютерная алгебра», «Алгебра», «Алгебраические системы», «Анализ эволюционных задач», «Вводный курс математики», «Геометрия», «Дискретная математика», «Дополнительные главы математического анализа», «Исследование операций и методы оптимизации», «Математическая логика», «Математический анализ», «Метрические пространства», «Основы теории решеток», «Основы универсальной алгебры», «Разработка электронных образовательных ресурсов», «Современные языки программирования», «Специализированные математические пакеты», «Теория алгоритмов», «Теория вероятностей и математическая статистика», «Теория функций действительного переменного», «Теория функций комплексного переменного», «Теория чисел», «Технологии Интернет-обучения», «Физика», «Численные методы», «Числовые системы», «Элементы общей алгебры», «Элементы статистической обработки данных», прохождения практик «Научно-исследовательская работа», «Практика по получению первичных профессиональных умений и навыков», «Практика по получению первичных умений и навыков научно-исследовательской деятельности», «Практика по получению профессиональных умений и опыта профессиональной деятельности».

## 3. Планируемые результаты обучения

В результате освоения дисциплины выпускник должен обладать следующими компетенциями:

- способностью использовать естественнонаучные и математические знания для ориентирования в современном информационном пространстве (ОК-3);
- способностью руководить учебно-исследовательской деятельностью обучающихся (ПК-12);
- владением математикой как универсальным языком науки, средством моделирования явлений и процессов; основными положениями классических разделов математической науки, базовыми идеями и методами математики, системой основных математических структур и аксиоматическим методом (СК-3).

**В результате изучения дисциплины обучающийся должен:**

### *знать*

- способы представления классических алгебраических структур на компьютере, границы применимости символьных вычислений на компьютере;
- основные методы и алгоритмы компьютерной алгебры;
- основные методы работы с многочленами в системе компьютерной алгебры;

### *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;
- применять основные алгоритмы, реализованные в системе компьютерной алгебры, для решения задач факторизации многочленов;

#### ***владеть***

- представлением о связи абстрактной алгебры и символьных вычислений на компьютере;
- приемами использования системы компьютерной алгебры для решения задач теории чисел;
- приемами использования системы компьютерной алгебры для решения задач факторизации многочленов.

#### **4. Общая трудоёмкость дисциплины и её распределение**

количество зачётных единиц – 3,

общая трудоёмкость дисциплины в часах – 108 ч. (в т. ч. аудиторных часов – 50 ч., СРС – 58 ч.),

распределение по семестрам – 10,

форма и место отчётности – аттестация с оценкой (10 семестр).

#### **5. Краткое содержание дисциплины**

Предмет компьютерной алгебры.

Предмет компьютерной алгебры. Символьные вычисления на компьютере. 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. Работа с конечными алгебраическими структурами на компьютере (группы подстановок, графы, квазигруппы).

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 многочленами над конечными полями и полем рациональных чисел.

Проблема факторизации многочленов (полиномов). Метод Кронекера. Строение конечных полей.

Факторизация полиномов над конечными полями. Алгоритм Берлекемпа. Случай

большого поля. Метрики поля рациональных чисел,  $p$ -адические числа, линейный и

квадратичный подъем. Факторизация полиномов над полем рациональных чисел.

Факторизация многочленов от нескольких переменных. Дискретное преобразование Фурье.

Системы алгебраических уравнений.

#### **6. Разработчик**

Лецко Владимир Александрович, кандидат педагогических наук, доцент кафедры алгебры, геометрии и математического анализа.