

# 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», «Дифференциальные уравнения», «Дополнительные главы математического анализа», «Компьютерное моделирование», «Математическая логика», «Математический анализ», «Операционная система Linux», «Основы искусственного интеллекта», «Основы универсальной алгебры», «Перспективные направления искусственного интеллекта», «Перспективные направления компьютерного моделирования», «Построение Windows-сетей», «Разработка Flash-приложений», «Разработка интернет-приложений», «Разработка электронных образовательных ресурсов», «Разработка эффективных алгоритмов», «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», 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».

Освоение данной дисциплины является необходимой основой для последующего изучения дисциплин «Исследование операций и методы оптимизации», «Метрические пространства», «Основы теории решеток», «Элементы общей алгебры», «Элементы статистической обработки данных», прохождения практики «Преддипломная практика».

## 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**

- строение конечных полей;
- свойства конечных полей, позволяющие осуществить эффективную факторизацию

полиномов над ними;  
– основные методы факторизации полиномов над полем рациональных чисел;

#### ***уметь***

– представлять конечные поля на компьютере;  
– реализовывать алгоритм Берлекэмпа;  
– применять алгоритмы, реализованные в системе компьютерной алгебры, для решения задач факторизации многочленов;

#### ***владеть***

– методами вычислений в конечных полях на компьютере;  
– приемами оценки вычислительной сложности задач факторизации полинома над тем или иным конечным полем;  
– приемами использования системы компьютерной алгебры для работы с полиномами над полем рациональных чисел.

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

количество зачётных единиц – 3,  
общая трудоёмкость дисциплины в часах – 108 ч. (в т. ч. аудиторных часов – 14 ч., СРС – 90 ч.),  
распределение по семестрам – 6 курс, зима,  
форма и место отчётности – аттестация с оценкой (6 курс, зима).

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

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 Берлекэмпа. Реализация алгоритма Берлекэмпа. Случай полей большой характеристики

Работа с многочленами над полем рациональных чисел и его конечными расширениями. Проблема факторизации многочленов в зависимости от поля, над которым ведется разложение. Метод Кронекера. Обобщение метода Кронекера на случай полиномов нескольких переменных. Метрики поля рациональных чисел,  $p$ -адические числа, линейный и квадратичный подъем. Факторизация полиномов над полем рациональных чисел. Алгоритмы факторизации на основе выбора малого вектора в решетке. Дискретное преобразование Фурье. Системы алгебраических уравнений. Понятие о базисах Грёбнера. Алгоритм Бухбергера.

### **6. Разработчик**

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