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», «Алгебра», «Анализ эволюционных задач», «Вводный курс математики», «Геометрия», «Дискретная математика», «Дифференциальные уравнения», «Дополнительные главы математического анализа», «Логическое введение в математику», «Математическая логика», «Математический анализ», «Разработка электронных образовательных ресурсов», «Теория алгоритмов», «Теория вероятностей и математическая статистика», «Теория функций действительного переменного», «Теория чисел», «Технологии Интернет-обучения», «Физика», «Числовые системы», прохождения практик «Исследовательская практика», «Практика по получению первичных профессиональных умений и навыков», «Практика по получению профессиональных умений и опыта профессиональной деятельности».
Освоение данной дисциплины является необходимой основой для последующего изучения дисциплин «Алгебраические системы», «История математики», «История становления математики», «Метрические пространства», «Основы универсальной алгебры», «Элементы статистической обработки данных», прохождения практик «Практика по получению профессиональных умений и опыта профессиональной деятельности», «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-1).

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 фаторизации 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 – 2,
общая трудоёмкость дисциплины в часах – 72 ч. (в т. ч. аудиторных часов – 10 ч., СРС – 58 ч.),
распределение по семестрам – 4 курс, лето,
форма и место отчётности – зачёт (4 курс, лето).

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 с 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, р-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.