ОСНОВЫ КОМПЬЮТЕРНОЙ АЛГЕБРЫ

1. Цель освоения дисциплины

Сформировать систему общекультурных, профессиональных и специальных компетенций будущего педагога путем изучения современных методов и алгоритмов в области компьютерной алгебры.

2. Место дисциплины в структуре ОПОП

Дисциплина «Основы компьютерной алгебры» относится к вариативной части блока дисциплин и является дисциплиной по выбору.
Для освоения дисциплины «Основы компьютерной алгебры» обучающиеся используют знания, умения, способы деятельности и установки, сформированные в ходе изучения дисциплин «Введение в теорию колец и модулей», «Графы и их приложения», «Исследование операций», «Логические вопросы алгебры», «Преподавание математики в учреждениях профессионального образования», «Проектирование содержания математических дисциплин в профессиональном образовании», «Теория алгебраических систем», «Теория групп», «Теория решеток», прохождения практики «Практика по получению профессиональных умений и опыта профессиональной деятельности (Педагогическая)».

3. Планируемые результаты обучения

В результате освоения дисциплины выпускник должен обладать следующими компетенциями:
– способностью проводить самостоятельные научные исследования по одному или нескольким направлениям универсальной алгебры, теории чисел, дискретной математики и их приложениям; внедрять в образовательный процесс полученные результаты собственных исследований или наиболее значимые результаты по направлениям, близким к научным интересам магистранта (СК-1).

В результате изучения дисциплины обучающийся должен:

знать
– способы представления классических алгебраических структур на компьютере, границы применимости символьных вычислений на компьютере;
– основные принципы работы с конечными алгебраическими структурами на компьютере;
– основные методы работы с многочленами в системе компьютерной алгебры;

уметь
– решать с использованием математических пакетов базовые задачи, относящиеся к компьютерной алгебре;
– реализовывать алгоритм разбиения конечных алгебраических структур, на классы изоморфных;
– 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 многочленовЖ реализовывать алгоритм Бухбергера;

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 – 4,
общая трудоёмкость дисциплины в часах – 144 ч. (в т. ч. аудиторных часов – 30 ч., СРС – 114 ч.),
распределение по семестрам – 4,
форма и место отчётности – зачёт (4 семестр).

5. Краткое содержание дисциплины

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 системами на компьютере.
Реализация конечных алгебраических систем на компьютере. Работа с группами подстановок и группами, заданными образующими и определяющими соотношениями. Перебор некоторых конечных алгебраических систем (квазигруппы, лупы, топологии, топологические группы…). Проблема изоморфизма конечных систем. Распределение конечных алгебраических систем на классы изоморфных.

Арифметика целых чисел на компьютере.
Сравнение, сложение, вычитание и умножение целых чисел в компьютерной алгебре. Деление с остатком. Сложение 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. Тесты простоты APRT CL и ECPP. Классические и современные алгоритмы факторизации натуральных чисел: метод Ферма; ро-метод Полларда; метод Ленстры; 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 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. Базисы Гребнера. Алгоритм Бухбергера.

6. Разработчик

Лецко Владимир Александрович, кандидат педагогических наук, доцент кафедры алгебры, геометрии и математического анализа ФГБОУ ВО «ВГСПУ».