СПИСОК КЛЮЧЕВЫХ ТЕМ, ЗНАНИЕ КОТОРЫХ НЕОБХОДИМО ДЛЯ ПОСТУПЛЕНИЯ НА МАГИСТЕРСКУЮ ПРОГРАММУ «МАТЕМАТИЧЕСКОЕ И ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ИНФОРМАЦИИ»

1. Определение группы (подгруппы), примеры. Разложение группы на смежные классы. Теорема Лагранжа. Порядок элемента конечной группы.
2. Группы подстановок, симметрическая группа. Цикловая структура подстановки и ее порядок. Представление подстановки в виде произведения транспозиций, четные и нечетные подстановки. Знакопеременная группа. Представление четной подстановки в виде произведения 3-циклов.
3. Гомоморфизм и изоморфизм групп, примеры. Нормальный делитель, ядро гомоморфизма. Теоремы о гомоморфизмах.
4. Определения кольца, поля, примеры. Делители нуля, обратимые элементы. Кольцо многочленов над полем. Теорема Безу. Критерий неприводимости многочленов второй и третьей степени.
5. Кольцо целых чисел. Делимость и ее свойства. Наибольший общий делитель. Алгоритм Евклида. Критерий взаимной простоты двух чисел. Кольцо вычетов.
6. Конечное поле, характеристика конечного поля и ее свойства. Число элементов конечного поля. Мультипликативная группа конечного поля, теорема Ферма.
7. Функции алгебры логики. Теорема о совершенной ДНФ. Теорема Жегалкина о представимости функций алгебры логики полиномами. Быстрый алгоритм построения полинома Жегалкина для функции алгебры логики.
8. Графы. Деревья, свойства деревьев. Остовное дерево графа. Алгоритм построения кратчайшего остовного дерева графа.
9. Детерминированные функции. Ограниченно-детерминированные функции. Задание ограниченно-детерминированных функций каноническими уравнениями. Операция суперпозиции. Замкнутость множества ОД-функций относительно операций суперпозиции.
10. Конечный автомат. Эквивалентность состояний автомата. Проверка эквивалентности состояний автомата, теорема Мура о длине слова, проверяющего эквивалентность состояний конечного автомата. Пример достижимости оценки в теореме Мура.
11. Алгоритм Карацубы и алгоритм Тоома для умножения чисел. Алгоритм Штрассена для умножения матриц. Оценки их сложности.
12. Классы P и NP. NP-трудные и NP-полные задачи. Теорема Кука о полноте задачи о выполнимости КНФ. Некоторые NP-полные задачи (3-КНФ, КЛИКА, НЕЗАВИСИМОЕ МНОЖЕСТВО, ВЕРШИННОЕ ПОКРЫТИЕ). Полиномиальность задачи о выполнимости 2-КНФ.

СПИСОК ЛИТЕРАТУРЫ

1. Применко Э.А. Алгебраические основы криптографии. М: Либроком, 2013 – 288
2. Алексеев В.Б. Введение в теорию сложности алгоритмов. М.: Изд-во ф-та ВМК МГУ им. М.В. Ломоносова, 2002.
3. Алексеев В.Б. Лекции по дискретной математике. М.: Инфра-М, 2012.
4. Гаврилов Г.П., Сапоженко А.А. Задачи и упражнения по дискретной математике. М.: Физматлит, 2004.
5. Сапоженко А.А. Некоторые вопросы сложности алгоритмов. М.: Изд-во ф-та ВМК МГУ им. М.В. Ломоносова, 2001.
6. Яблонский С.В. Введение в дискретную математику. М.: Высшая школа, 2001.