Экзаменационная программа по курсу «Математические основы защиты информации», направление подготовки ФИИТ, 2 курс, 2 семестр 2019–2020 учебного года

Элементы теории чисел. Аксиома полной упорядоченности. Лемма о делении с остатком. Функции «пол» и «потолок». Отношение делимости. Наибольший общий делитель, теорема существования и единственности, следствия. Линейное представление наибольшего общего делителя. Свойства наибольшего общего делителя. Алгоритм Евклида. Алгоритм нахождения линейного представления наибольшего общего делителя. Взаимно простые числа; свойства взаимно простых чисел; описание делителей произведения двух взаимно простых чисел. Наименьшее общее кратное (определение, теорема существования и единственности). Теорема о равенстве $ab = (a,b)[a,b]$.

Простые числа. Теорема о наименьшем отличном от единицы делителе числа, бесконечность множества простых чисел. Свойства простых чисел. Основная теорема арифметики (существование и единственность разложения числа $n > 1$ на простые множители). Каноническое разложение числа, общий вид делителей числа.

Сравнения. Свойства сравнений, полная система вычетов. Мультипликативные функции. Свойства мультипликативных функций. Функция Мебиуса, ее мультипликативность. Функция Эйлера, мультипликативность функции Эйлера. Функции e и I. Произведение Дирихле. Преобразование Дирихле. Мультипликативность произведения Дирихле мультипликативных функций, следствия. Преобразования Дирихле функции Мебиуса и функций $f(n) = n^s$. Формула обращения Мебиуса. Следствие о мультипликативности арифметической функции с мультипликативным преобразованием Дирихле. Приведенная система вычетов. Функция Эйлера (определение, формула для вычисления функции Эйлера). Теоремы Эйлера и Ферма. Теорема существования и единственности решения сравнения первой степени, алгоритм решения. Система сравнений первой степени с одной неизвестной.

Алгебраические системы с одной операцией. Бинарная операция, таблица Кэли. Коммутативность и ассоциативность. Моноид. Единственность единичного элемента. Мультипликативная и аддитивная запись. Примеры моноидов.

Группа, аксиоматика, единственность обратного элемента, свойства обратного элемента. Целые степени элемента группы. Конечные и бесконечные группы, порядок группы. Примеры групп. Порядок элемента группы, свойства порядка (условия, равносильные конечности порядка; порядок элемента конечной группы; порядок степени элемента; порядок

произведения элементов конечного порядка). Подгруппы, примеры подгрупп. Критерии того, что подмножество является подгруппой.

Циклические группы, примеры циклических групп. Примеры нециклических групп. Подгруппа $< a >$ связь ее порядка с порядком элемента $a,$ альтернативное определение цикличности группы. Критерий цикличности конечной группы. Теорема о цикличности подгрупп циклической группы. Теорема о подгруппах бесконечной циклической группы, следствие о подгруппах группы $\mathbb{Z}_n$.

Гомоморфизм, свойства гомоморфизмов. Ядро гомоморфизма (определение, теорема, критерий инъективности гомоморфизма). Образ гомоморфизма (определение, теорема, критерий сюръективности гомоморфизма). Изоморфизм. Критерий того, что гомоморфизм является изоморфизмом. Теоремы об изоморфизме для конечной и бесконечной циклической группы.

Операции с подмножествами элементов группы, свойства этих операций. Отношение эквивалентности, определяемое подгруппой, левый смежный класс. Правый смежный класс. Равномощность двух смежных классов. Равномощность множества всех левых смежных классов и множества всех правых смежных классов, индекс подгруппы. Теорема Лагранжа, следствия. Теорема о подгруппах конечной циклической группы. Следствия. Критерий того, что группа не имеет собственных подгрупп. Нормальные подгруппы; критерий нормальности подгруппы. Лемма о произведении смежных классов по нормальной подгруппе. Факторгруппа, теорема о каноническом гомоморфизме, теорема о гомоморфизмах, следствие об изоморфных группах.

Прямое произведение групп, элементарные свойства.

Экспонента группы, свойства экспоненты (включая утверждения: существование в конечной коммутативной группе G элемента, для которого $|a| = \exp(G)$; критерий цикличности конечной коммутативной группы; критерий цикличности прямого произведения конечных коммутативных групп).

Литература

1, В.С. Пилиди. Математические основы защиты информации.

2. И.М. Виноградов. Основы теории чисел.

3. Б.Л. ван дер Варден. Алгебра.