ЭКЗАМЕНАЦИОННАЯ ПРОГРАММА ПО КУРСУ
«МАТЕМАТИЧЕСКИЕ ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ»,
НАПРАВЛЕНИЕ ПОДГОТОВКИ «ФИИТ»,
2 КУРС, 1 СЕМЕСТР 2015–2016 УЧЕБНОГО ГОДА

ЭЛЕМЕНТЫ ТЕОРИИ ЧИСЕЛ. Аксиома полной упорядоченности. Лемма о делении с остатком. Функции «пол» и «потолок». Отношение делимости. Множества $\mathcal{D}(a)$, $\mathcal{D}(a,b)$ и их свойства. Наибольший общий делитель, теорема существования и единственности, следствия о единственности наибольшего общего делителя. Линейное представление наибольшего общего делителя. Свойства наибольшего общего делителя. Алгоритм Евклида. Алгоритм нахождения линейного представления наибольшего общего делителя. Сложность алгоритма Евклида. Взаимно простые числа; теорема о свойствах, равносильных взаимной простоте; свойства взаимно простых чисел; описание делителей произведения двух взаимно простых чисел. Наименьшее общее кратное (определение, теорема существования и единственности). Теорема о равенстве

$$[a_1,\ldots,a_n,a_{n+1}]=\big[[a_1,\ldots,a_n],a_{n+1}]\big].$$

Теорема о равенстве $ab=(a,b)[a,b]$.

Определение и элементарные свойства простых чисел (теорема о наименьшем отличном от единицы делителе числа, следствие теоремы, решето Эратосфена, бесконечность множества простых чисел). Свойства простых чисел ($\forall a$ $p\mid a$ или $(a,p)=1$; $p\mid ab \Rightarrow p\mid a$ или $p\mid b$; $p\mid q \Rightarrow p=q$). Основная теорема арифметики (существование и единственность разложения числа $n>1$ на простые множители). Каноническое разложение числа, общий вид делителей числа, вычисление значения функции $\nu(n)$. Функция ord_p, её свойства. Теорема о соотношении $n\mid C_n^k$. Вычисление значения $\operatorname{ord}_p(n!)$ (лемма и теорема).

Мультипликативные функции. Свойства мультипликативных функций. Функция Мебиуса. Мультипликативность функции Мебиуса. Преобразование Дирихле. Функции e и I. Мультипликативность произведения Дирихле мультипликативных функций, следствие о мультипликативности преобразования Дирихле мультипликативной функции, следствие о вычислении преобразования Дирихле мультипликативной функции. Преобразования Дирихле функции Мебиуса и функций $f(n)=n^s$. Функция Эйлера (определение, вычисление значения $\varphi(p^k)$, теорема о равенстве $\sum_{d\mid n}\varphi(d)=n$, следствие о мультипликативности и формуле для вычисления функции Эйлера). Совершенные числа, критерий совершенности четного числа. Формула для вычисления произведения всех делителей данного числа, «мультипликативно совершенные» числа, критерий.

Сравнения. Свойства сравнений, классы чисел по данному модулю. Полная и приведенная системы вычетов. Линейные преобразования полной и приведенной систем вычетов (лемма и теорема). 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 (включая: условия, равносильные конечности порядка; порядок элемента конечной группы; порядок степени элемента; порядок произведения элементов конечного порядка). Подгруппы, примеры подгрупп. Совпадение единичных элементов группы и подгруппы. Критерии того, что подмножество является подгруппой.

Циклические группы, примеры циклических групп. Примеры нециклических групп. Подгруппа $\langle a \rangle$, связь её 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 (исчерпываются попарно различными циклическими подгруппами $\langle a^k \rangle$, $k = 0,\ 1,\ \ldots$). Следствие о подгруппах группы $\mathbb{Z}$.

Гомоморфизм, свойства гомоморфизмов. Ядро гомоморфизма (определение, теорема, критерий инъективности гомоморфизма). Образ гомоморфизма (определение, теорема, критерий сюръективности гомоморфизма). Изоморфизм. Критерий того, что гомоморфизм является изоморфизмом.

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 ($|G| = |G:H| \cdot |H|$), следствие о цикличности группы простого порядка. Критерий того, что группа не имеет собственных подгрупп. Теорема о подгруппах конечной циклической группы. Нормальные подгруппы; критерий нормальности подгруппы. Факторгруппа, теорема о гомоморфизмах.

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. И.М. Виноградов. Основы теории чисел.

2. Б.Л. ван дер Варден. Алгебра.