ЭКЗАМЕНАЦИОННАЯ ПРОГРАММА ПО КУРСУ
«МАТЕМАТИЧЕСКИЕ ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ»,
НАПРАВЛЕНИЕ ПОДГОТОВКИ «ФИИТ»,
2 КУРС, 2 СЕМЕСТР 2016–2017 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. Линейное представление наибольшего общего делителя. Свойства наибольшего общего делителя. Алгоритм Евклида. Алгоритм нахождения линейного представления наибольшего общего делителя. 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 $ab=(a,b)[a,b]$.

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. Функции e и I. Произведение Дирихле. Преобразование Дирихле. 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 $f(n)=n^s$. Формула обращения Мебиуса. Следствие о мультипликативности арифметической функции с мультипликативным преобразованием Дирихле. Полная и приведенная системы вычетов. Функция Эйлера. Вычисление $\varphi(p)$, $\varphi(p^k)$. Дополнения о НОД: свойства

$$(ac,b)=(a,b),\ (ua,ub)=u(a,b),\ (ab,c)=(a,c)(b,c).$$

Теорема о суммах вида $bu+av$. Следствие о мультипликативности функции Эйлера, формула для вычисления $\varphi(n)$.

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.

Совершенные числа, критерий совершенности четного числа. Формула для вычисления произведения всех делителей данного числа, «мультипликативно совершенные» числа, критерий.

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. Теорема (конечная циклическая группа G порядка n изоморфна U_n). Следствие. Теорема (бесконечная циклическая группа G изоморфна аддитивной группе $\mathbb{Z}$). Следствие. Примеры неизоморфных групп.

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 ($|G| = |G:H| \cdot |H|$), 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).

КОЛЬЦА. Определение, примеры колец. Обратимые элементы, мультипликативная группа кольца. Делители нуля, необратимость делителя нуля. Поле, примеры полей, теорема (конечное коммутативное кольцо без делителей нуля является полем), следствие (критерий того, что кольцо $\mathbb{Z}_n$ является полем).

Подкольцо, критерий того, что подмножество является подкольцом. Гомоморфизм колец.

Кольцо многочленов над произвольным полем. Деление с остатком. Нормированные многочлены, обратимые элементы кольца многочленов. Делимость многочленов, свойства отношения делимости. Наибольший общий делитель (определение, теорема существования, следствие о единственности нормированного НОД, следствие о линейном представлении НОД). Взаимно простые многочлены. Корень многочлена, кратность корня. Приводимые и неприводимые многочлены. Свойства неприводимых многочленов. Теорема о разложении многочлена на неприводимые множители. Каноническое разложение многочлена. Теорема о числе корней многочлена степени n, следствия. Теорема Вильсона. Неприводимые многочлены над полями $\mathbb{C}$ и $\mathbb{R}$. Неприводимость многочленов с рациональными коэффициентами (лемма Гаусса, теорема Гаусса, признак Эйзенштейна). Неприводимые многочлены в случае конечного поля. Производная многочлена. Критерий простоты корня многочлена.

Литература

1. И.М. Виноградов. Основы теории чисел.
2. Б.Л. ван дер Варден. Алгебра.