ОДМ 1 курс 1 семестр 2017.

I. Знать определения. Необходимо знать определения перечисленных понятий, уметь ими оперировать и приводить соответствующие примеры.

(1) Прямое произведение множеств.

(2) Функция (отображение).

(3) Инъективное, сюръективное, биективное отображение.

(4) Тождественное отображение; обратное отображение.

(5) Характеристическая функция подмножества.

(6) Композиция отображений.

(7) Счетное множество.

(8) Несчетное множество.

(9) Отношение.

(10) Отношение эквивалентности. Классы эквивалентности.

(11) Отношение порядка.

(12) Перестановки из n элементов.

(13) Умножение (композиция) перестановок.

(14) Два способа записи перестановок.

(15) Цикловый тип перестановки.

(16) Порядок перестановки.

(17) Четность перестановки.

(18) Деление целых чисел с остатком.

(19) Сравнимость целых чисел по модулю n.

(20) Множество остатков (вычетов по модулю n) $\mathbb{Z}_n$.

(21) Определение операций сложения и умножения в $\mathbb{Z}_n$.

(22) Обратимый элемент в $\mathbb{Z}_n$.

(23) Делитель нуля в $\mathbb{Z}_n$.

(24) Нильпотентный и идемпотентный элемент в $\mathbb{Z}_n$.

(25) Бинарная операция на множестве.

(26) Определение группы, абелевой группы, кольца. Коммутативное ассоциативное кольцо с единицей.

(27) Прямое произведение колец.

(28) Обратимые элементы, делители нуля, нильпотентные и и идемпотентные элементы в коммутативном ассоциативном кольце с единицей.

(29) Понятие изоморфизма колец.

(30) Порядок элемента в $\mathbb{Z}_n$ по сложению и по умножению.

(31) Функция Эйлера.

(32) Символ Лежандра.

(33) Число сочетаний C_n^k — количество k-элементных подмножеств множества из n элементов.

II. Уметь.

(1) Приводить примеры ко всем понятиям части "Знать".

(2) Доказывать различные утверждения методом полной математической индукции.

(3) Доказывать свойства операций над множествами (объединение, пересечение, дополнение, разность) и проверять аналогичные тождества с использованием этих операций.

(4) Устанавливать взаимно однозначное соответствие между различными счетными множествами ($\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Z} \times \mathbb{Z}$, $\mathbb{Q}$ и т.д.).

(5) Перемножать перестановки.

(6) Представлять перестановку в виде произведения независимых циклов, определять ее четность и порядок.

(7) Производить вычисления в арифметике остатков $\mathbb{Z}_n$.

(8) Перечислять обратимые элементы в $\mathbb{Z}_n$ и вычислять обратные к ним.

(9) Вычислять значения функции Эйлера.

(10) Находить порядки элементов в $\mathbb{Z}_n$ по сложению и (для обратимых элементов) по умножению.

(11) Находить идемпотентные элементы в $\mathbb{Z}_n$.

(12) Пользоваться китайской теоремой об остатках, т.е. явно выписывать формулы изоморфизма $\mathbb{Z}_{mn}$ прямому произведению колец $\mathbb{Z}_m$ и $\mathbb{Z}_n$ и обратного изоморфизма.

(13) Решать простейшие комбинаторные задачи.

III. Результаты. Необходимо знать формулировки перечисленных перечисленных результатов и уметь ими пользоваться при решении задач. Для получения оценки выше "уд" необходимо также уметь эти результаты доказывать.

(1) Композиция двух сюръективных/инъективных/биективных отображений также является сюръективным/инъективным/биективным отображением.

(2) Необходимое и достаточное условие существования обратного отображения.

(3) Задание отношения эквивалентности на множестве равносильно заданию разбиения его на непересекающиеся подмножества. Классы эквивалентности.

(4) Биекция между множеством подмножеств множества Ω и множеством характеристических функций на Ω.

(5) Характеристические функции пересечения, дополнения и объединения множеств. ($\chi_{A\cap B} = \chi_A \cdot \chi_B$, $\chi_{\Omega\setminus A} = 1 - \chi_A$, $\chi_{A\cup B} = \chi_A + \chi_B - \chi_A \cdot \chi_B$.)

(6) Формула включений-исключений.

(7) Мощность множества отображений из множества X в множество, Y, если $|X| = n$ и $|Y| = m$.

(8) Мощность множества инъективных отображений из множества X в множество, Y, если $|X| = n$ и $|Y| = m$ и $n \leq m$.

(9) Мощность множества $S(X)$ биективных отображений из множества X в себя, если $|X| = n$.

(10) Множество бесконечно тогда и только тогда, когда оно равномощно своему собственному подмножеству.

(11) Любое бесконечное множество содержит счетное подмножество.

(12) Любое бесконечное подмножество счетного множества счетно.

(13) Прямое произведение счетных множеств счетно.

(14) Объединение любого бесконечного множества со счетным равномощно ему самому.

(15) Множество конечных слов в конечном алфавите счетно.

(16) Множество последовательностей из 0 и 1 несчетно.

(17) $\mathbb{Q}$ счетно.

(18) $\mathbb{R}$ несчетно.

(19) Множество подмножеств множества Ω не равномощно Ω.

(20) Теорема Кантора-Бернштейна (без доказательства).

(21) Представление перестановки в виде произведения независимых циклов. Перестановочность независимых циклов.

(22) Представление перестановки в виде произведения транспозиций.

(23) При умножении на транспозицию четность перестановки меняется.

(24) Число четных перестановок равно числу нечетных.

(25) Представление цикла в виде произведения транспозиций. Четность цикла в зависимости от его длины.

(26) Определение четности перестановки по ее цикловому типу.

(27) Сопоставление перестановке матрицы, доказательство согласованности этого сопоставления с умножением матриц и перестановок; интерпретация четнности перестановки как определителя сопоставляемой матрицы.

(28) Вычитание в арифметике остатков $\mathbb{Z}_n$.

(29) Диофантово уравнение $ax + by = c$. Необходимое и достаточное условие существования решения. Общее решение. Сведение к случаю уравнения $ax + by = 1$.

(30) Необходимое и достаточное условие обратимости остатка $\bar{a} \in \mathbb{Z}_n$.

(31) Необходимое и достаточное условие того, что остаток $\bar{a} \in \mathbb{Z}_n$ является делителем нуля.

(32) Доказательство корректности определения порядка элемента $\bar{a} \in \mathbb{Z}_n$ по сложению: если в последовательности $\bar{0}$, $\bar{a}$, $\bar{a}+\bar{a}$, $\bar{a}+\bar{a}+\bar{a}$, ..., $\underbrace{\bar{a}+\bar{a}+\ldots+\bar{a}}_{k-1 \text{ слагаемое}}$ все элементы различны, а $\underbrace{\bar{a}+\bar{a}+\ldots+\bar{a}}_{k \text{ слагаемых}}$ совпадает с одним из предыдущих, то $\underbrace{\bar{a}+\bar{a}+\ldots+\bar{a}}_{k \text{ слагаемых}} = \bar{0}$.

(33) Если для $\bar{a} \in \mathbb{Z}_n$ $\underbrace{\bar{a}+\bar{a}+\ldots+\bar{a}}_{k \text{ слагаемых}} = \bar{0}$, то k делится на порядок остатка $\bar{a}$ по сложению.

(34) Порядок по сложению остатка $\bar{a} \in \mathbb{Z}_n$ является делителем n.

(35) Доказательство корректности определения порядка элемента $\bar{a} \in \mathbb{Z}_n^*$ по умножению: если в последовательности $\bar{1}$, $\bar{a}$, $\bar{a}^2$, $\bar{a}^3$, ..., $\bar{a}^{k-1}$ все элементы различны, а $\bar{a}^k$ совпадает с одним из предыдущих, то $\bar{a}^k = \bar{1}$.

(36) Если для $\bar{a} \in \mathbb{Z}_n$ $\bar{a}^k = \bar{1}$, то k делится на порядок остатка $\bar{a}$ по умножению.

(37) Малая теорема Ферма.

(38) Теорема Эйлера.

(39) Теорема Вильсона.

(40) Порядок по умножению обратимого остатка $\bar{a} \in \mathbb{Z}_n$ является делителем значения функции Эйлера $\varphi(n)$.

(41) Китайская теорема об остатках.

(42) Нахождение идемпотентных остатков с помощью решения диофантова уравнения $ax + by = 1$.

(43) Число идемпотентных остатков в $\mathbb{Z}_n$, где $n = p_1^{k_1} p_2^{k_2} \ldots n = p_s^{k_s}$, $p_1, \ldots, p_s$ — различные простые числа.

(44) Явная формула для биекции в китайской теореме об остатках (через идемпотентные остатки).

(45) Условия представимости кольца остатков $\mathbb{Z}_n$ в виде прямого произведения колец.

(46) Кольцо изоморфно прямому произведению колец тогда и только тогда, когда оно содержит идемпотентые элементы.(Доказательство только в одну сторону.)

(47) Кольцо $\mathbb{Z}_{p^m}$ нельзя представить в виде прямого произведения колец (p — простое число).

(48) Решение уравнения $x^2 = 1$ в кольце $\mathbb{Z}_{p^m}$, где p — простое число. ($p = 2$ надо рассмотреть отдельно!)

(49) Описание множества решений уравнения $x^2 = 1$ прямом произведения колец. Решения этого уравнения в $\mathbb{Z}_n$.

(50) Описание обратимых элементов прямого произведения колец и вывод мультипликативности функции Эйлера.

(51) Мультипликативность функции Эйлера.

(52) Вычисление значения функции Эйлера $\varphi(p^m)$, где p — простое число.

(53) Формула для символа Лежандра $\left(\begin{array}{c} a \\ p \end{array}\right) = \bar{a}^{\frac{p-1}{2}}$. Мультипликативность символа Лежандра. (p — нечетное простое число.)

(54) При каких простых значениях p остаток $-\bar{1}$ является квадратом в $\mathbb{Z}_p$?

(55) Доказательство формулы $C_n^k + C_n^{k+1} = C_{n+1}^{k+1}$.

(56) Бином Ньютона.

(57) Свойства треугольника Паскаля.

(58) Формула для вычисления биномиальных коэффициентов C_n^k.

(59) $C_n^0 + C_n^1 + C_n^2 + \ldots + C_n^{n-11} + C_n^n = 2^n$.

(60) $C_n^0 - C_n^1 + C_n^2 - \ldots + (-1)^n C_n^n = 0$.

(61) $C_n^0 + C_{n+1}^1 + C_{n+2}^2 + \ldots + C_{n+k}^k = C_{n+k+1}^k$.

(62) Число разбиений натурального числа n в сумму k целых неотрицательных слагаемых.

(63) Число разбиений натурального числа n в сумму k натуральных слагаемых.