

# Теоретическая информатика

## Список тем и вопросов к экзамену

### **Элементы теории множеств**

▼ Множества. Способы задания множеств. Операции над множествами (объединение, пересечение, дополнение, разность, симметрическая разность) и их свойства. Диаграммы Эйлера — Венна. Прямое произведение. Характеристический вектор множества. Характеристическая функция множества. Мощность множества и её связь с характеристической функцией.

**Вопросы для самоконтроля:** Что может выступать в качестве элементов множества? Что такое пустое множество? Что такое универсальное множество? Как выражается характеристическая функция  $\chi_{A \Delta B}(x)$  через  $\chi_A(x)$  и  $\chi_B(x)$ ? Чему равна мощность  $|\emptyset|$ ? А мощность  $|\{\emptyset\}|$ ? Чему равна мощность  $|A \times B|$ ? Как выглядит  $A \times B$ , если  $A = \{1, 2\}$ ,  $B = \{1, 3\}$ ? Что представляет собой прямое произведение множеств точек двух отрезков? Отрезка и прямоугольника? Отрезка и окружности?

▼ Подмножества. Собственные и нетривиальные подмножества.

**ВдСК:** Как соотносятся  $\chi_A(x)$  и  $\chi_B(x)$ , если  $A \subseteq B$ ? В каком случае справедливо равенство  $\chi_{A \setminus B}(x) = \chi_A(x) - \chi_B(x)$ ? В чём разница между  $(A \subseteq B)$  и  $(A \in B)$ ? Какие из этих утверждений справедливы:  $\emptyset \subseteq \mathbb{N}$ ,  $\emptyset \in \mathbb{N}$ ,  $\emptyset \subseteq \emptyset$ ,  $\emptyset \in \emptyset$ ? Сколько собственных подмножеств у множества мощностью 10? А сколько нетривиальных? Подмножеств какой мощности среди них больше всего?

▼ Бинарные отношения на множестве. Свойства бинарных отношений.

**ВдСК:** Сколько можно задать бинарных отношений на множестве мощностью  $n$ ? Сколько рефлексивных? Иррефлексивных? Симметричных? Какими свойствами обладает отношение строгого включения?

▼ Отображения. Типы отображений. Элементарные функции как отображения. Композиция отображений. Тождественное отображение. Обратное отображение и условие его существования.

**ВдСК:** Сколько можно задать отображений из множества мощностью  $a$  в множество мощностью  $b$ ? А сколько биекций? Как должны соотноситься мощности конечных множеств  $A$  и  $B$ , чтобы можно было задать инъективное отображение  $f : A \rightarrow B$ ? А сюръективное? Является ли отображение  $n! : \mathbb{N}_0 \rightarrow \mathbb{N}$  инъективным, сюръективным? Является ли отображение  $\det M : M_{n \times n} \rightarrow \mathbb{R}$  инъективным, сюръективным? Укажите такие множества  $X$  и  $Y$ , чтобы для отображения  $\sin x : X \rightarrow Y$  существовало обратное.

▼ Подстановки на конечном множестве. Формы записи подстановки: двухэтажная, цикловая. Умножение подстановок. Порядок подстановки.

**ВдСК:** Коммутативно ли умножение подстановок? Как найти подстановку, обратную к данной? Сколько на множестве  $\{1, 2, \dots, 8\}$  подстановок? Сколько из них переводят элемент 3 в элемент 7, а элемент 5 оставляют на месте? Сколько существует способов записать подстановку  $(1 \ 5 \ 6)(2 \ 3 \ 4)(7 \ 8)$  в виде произведения независимых циклов? Сколько подстановок на множестве мощностью 8 может быть представлено в виде произведения двух независимых циклов: длины 3 и 5?

▼ Принцип включения-исключения.

**ВдСК:** Сколько слагаемых (то есть различных мощностей) окажется в формуле включения-исключения для 10 множеств, если раскрыть все суммы?

### Основные комбинаторные понятия и схемы

► Два основных правила комбинаторики: правило суммы, правило произведения.

▼ Четыре основных схемы выборки: размещение с повторениями, размещение без повторений, сочетание с повторениями, сочетание без повторений. Перестановка как частный случай размещения.

**ВдСК:** Может ли в формуле сочетаний без повторений верхний индекс быть больше нижнего? А в формуле сочетаний с повторениями? Сколькими способами можно разложить 20 разных шаров по шести занумерованным мешкам? А 20 одинаковых шаров? А 10 белых, 15 чёрных и 20 синих шаров?

▼ Биномиальные коэффициенты и их свойства. Треугольник Паскаля. Бином Ньютона. Свёртка Вандермонда.

**ВдСК:** Чему равно  $C_0^0$ ? Чему равен  $(0!)$ ? При каком  $k$ , значение  $C_n^k$  максимально?

▼ Полиномиальные коэффициенты. Схема перестановки с повторениями.

**ВдСК:** Как раскрыть  $(a + b + c + d)^3$ ? Сколько слагаемых в этом многочлене?

### Основы теории чисел

▼ Делимость целых чисел. Остаток от деления и его свойства. Простые и составные числа. Собственные и тривиальные делители.

**ВдСК:** Является ли единица простым числом? Сколько чисел из диапазона [100, 2000] делится на 5? А из диапазона [-100, 2000]?

▼ Теоремы Евклида: о бесконечности количества простых чисел; о подряд идущих составных числах; о разложении числа на простые сомножители (основная теорема арифметики).

**ВдСК:** Сколько делителей у числа  $2^5 \cdot 3^2 \cdot 7$ ? Сколько нетривиальных?

▼ Наибольший общий делитель и наименьшее общее кратное. Взаимосвязь НОД и НОК. Взаимно простые числа. Функция Эйлера. Основное свойство НОД. Алгоритм Евклида. Расширенный алгоритм Евклида. Соотношение Безу.

**ВдСК:** Чему равен НОД( $0, n$ )? Какими свойствами обладает отношение взаимной простоты? Есть ли разница между утверждениями «НОД( $a, b, c$ ) = 1» и «числа  $a, b, c$  являются попарно взаимно простыми»? Если да, то какое утверждение является более «сильным»? Верно ли, что  $\text{НОД}(a, b, c) \cdot \text{НОК}(a, b, c) = a \cdot b \cdot c$ ? Чему равна функция Эйлера  $\varphi(1)$ ? При каких  $n$  значение  $\varphi(n)$  нечётно? При каких  $n$   $\varphi(n) = 2$ ?

### Модульная арифметика и алгебра

▼ Группа, кольцо, поле.

**ВдСК:** Является ли группой  $\langle \mathbb{N}, + \rangle$ ?  $\langle \mathbb{N}_0, + \rangle$ ?  $\langle \mathbb{Z}, + \rangle$ ?  $\langle \mathbb{Q}, + \rangle$ ?  $\langle \mathbb{Q}, \cdot \rangle$ ?  $\langle \mathbb{Q}^+, \cdot \rangle$ ? Что представляет собой симметрическая группа  $\mathbb{S}_n$ ? Является ли кольцом (если да — является ли также полем)  $\langle \mathbb{Z}, +, \cdot \rangle$ ?  $\langle \mathbb{Q}, +, \cdot \rangle$ ?  $\langle \mathbb{Q}^+, +, \cdot \rangle$ ?  $\langle \mathbb{R}, +, \cdot \rangle$ ?

▼ Множество (кольцо, поле) вычетов по модулю  $m$ . Арифметические операции в  $\mathbb{Z}_m$ . Нейтральный элемент (относительно сложения, умножения). Обратный элемент (по сложению, по умножению). Теорема об обратимости элемента по умножению.

**ВдСК:** Какие элементы входят в  $\mathbb{Z}_m$ ? Сколько элементов  $\mathbb{Z}_m$  обратимо по сложению? По умножению? А если  $m$  простое?

▼ Сравнимость чисел по модулю  $m$ . Операции над сравнениями.

**ВдСК:** В чём отличие сравнимости  $a \equiv b \pmod{m}$  от равенства  $a = b \pmod{m}$ ? Какими свойствами обладает отношение сравнимости? Как выглядят признаки делимости на 3, 9, 11?

- Теорема Эйлера. Малая теорема Ферма.
- Сравнения первой степени, алгоритм их решения.
- Системы сравнений первой степени. Метод последовательной подстановки. Китайская теорема об остатках.

### Системы счисления

► Позиционные (чистые и смешанные) и непозиционные системы счисления.

▼ Перевод целых чисел из десятичной системы в  $b$ -ричную и обратно.

**ВдСК:** Как записывается число  $b$  в  $b$ -ричной системе счисления?

▼ Представление дробей (обыкновенных и позиционных, конечных и периодических) в различных системах счисления.

**ВдСК:** Чему равно  $0.(9)$ ?

▼ Перевод чисел между системами с основаниями  $b$  и  $b^k$ .

**ВдСК:** Как быстро умножить или разделить число на  $b^k$  в  $b$ -ричной системе счисления?

► Арифметические операции в  $b$ -ричной системе счисления.