

**Федеральное государственное автономное образовательное учреждение
высшего образования
"Национальный исследовательский университет
"Высшая школа экономики"**

Факультет компьютерных наук
Департамент программной инженерии

**Рабочая программа дисциплины
Дискретная математика**

для образовательной программы «Программная инженерия»
направления подготовки 09.03.04 «Программная инженерия»
уровень бакалавр

Разработчики программы

Авдошин С.М., профессор, к.т.н. savdoshin@hse.ru

Дворянский Л.В., старший преподаватель, ldworzanski@hse.ru

Набебин А.А., доцент, к.ф.-м.н.

Одобрена на заседании департамента программной инженерии «___» 2017 г.
Руководитель департамента Авдошин С.М. _____

Утверждена Академическим советом образовательной программы
«___» 2017 г., № протокола _____

Академический руководитель образовательной программы
Шилов В.В. _____

Москва, 2017

*Настоящая программа не может быть использована другими подразделениями университета
и другими вузами без разрешения подразделения-разработчика программы.*

1 Область применения и нормативные ссылки

Настоящая программа учебной дисциплины «Дискретная математика» (1 год обучения) устанавливает минимальные требования к знаниям и умениям студента и определяет содержание и виды учебных занятий и отчетности.

Программа предназначена для преподавателей и учебных ассистентов, ведущих данную дисциплину, а также студентов образовательной программы «Программная инженерия» направления подготовки 09.03.04 «Программная инженерия» факультета компьютерных наук, изучающих обязательную дисциплину “Дискретная математика” (блок Б.ПЦ.Б – Базовая часть дисциплин профессионального цикла рабочего учебного плана на 2017-2018 учебный год).

Данная программа разработана в соответствии с

- Международным образовательным стандартом Software Engineering 2004. Curriculum Guidelines for Undergraduate Degree Programs in Software Engineering. <http://sites.computer.org/ccse/SE2004Volume.pdf>
- Международным образовательным стандартом Computer Science Curricula 2013. <http://www.acm.org/education/CS2013-final-report.pdf>
- Международным образовательным стандартом Software Engineering 2014. Curriculum Guidelines for Undergraduate Degree Programs in Software Engineering. <http://www.acm.org/binaries/content/assets/education/se2014.pdf>
- Международным профессиональным стандартом IEEE – SWEBOk Guide V3. <http://www.computer.org/portal/web/swebok>
- Международной моделью компетенций IEEE – SWECOM V1.0 <http://www.computer.org/web/peb/swecom>
- Федеральным государственным образовательным стандартом высшего образования по направлению подготовки 09.03.04 Программная инженерия (уровень бакалавриата) http://fgosvo.ru/uploadfiles/ProjFGOSVO3++/Bak3++/090304_В_3plus_04042017.pdf
- Образовательным стандартом НИУ ВШЭ по направлению подготовки 09.03.04 Программная инженерия (Уровень подготовки: Бакалавр) http://www.hse.ru/data/2015/05/20/1097268782/Бакалавриат_ОС_Программная%20инженерия.pdf
- Образовательной программой НИУ ВШЭ по направлению подготовки 09.03.04 Программная инженерия (Уровень подготовки: Бакалавр)
- Базовым учебным планом университета по направлению подготовки 09.03.04 Программная инженерия, утвержденным в 2017 г. <https://www.hse.ru/standards/plans/343935449/>
- Рабочим учебным планом университета по направлению подготовки 09.03.04 Программная инженерия, утвержденным в 2017 г. <https://www.hse.ru/standards/plans/343935449/>

2 Цель освоения дисциплины

Основной целью освоения дисциплины “Дискретная математика” является формирование понимания студентами ключевых положений информатики, математической логики и теории алгоритмов, необходимых для практического использования на последующих этапах обучения и в профессиональной сфере деятельности будущего специалиста.

С точки зрения практической составляющей курса, основной целью ставится изучение логических основ информатики и основных концепций, которые позволяют студентам получить базовое представление об эффективных способах разработки программного обеспечения. Речь здесь идет о формировании у студентов компетенций, связанных с базовыми понятиями, которые составляют основу программирования, и позволяют сделать процесс проектирования программ и программирования более легким и эффективным.

Предлагаемая дисциплина ориентирована на формирование у студентов навыков логического и алгоритмического мышления при реализации решения поставленной задачи в виде программы. При этом основной акцент в курсе делается на изучении основ информатики и базовые парадигмы программирования.

3 Компетенции обучающегося, формируемые в результате освоения дисциплины

В результате освоения дисциплины студент должен:

- Знать
 - базовые разделы информатики, математической логики и теории алгоритмов и их связь с программированием и другими науками;
 - принципы построения позиционных систем счисления, базовые идеи, определяющие алгоритмы перевода чисел из одной системы счисления в другую;
 - особенности представления числовой (целые и вещественные числа) и символьной информации в компьютере,
 - основные понятия логики высказываний и предикатов, их связь с теорией множеств;
 - замкнутые классы, полные системы и базисы логических функций, частично-определенные функции и их минимизация в заданных базисах;
 - принцип дедукции, метод резолюций формальный вывод, клаузальная логика, семантические сети;
 - алгоритм, и его свойства, формальное определение, способы записи; базовые канонические алгоритмические структуры;
 - алгоритмически неразрешимые задачи, меры и классы сложности алгоритмов;
 - основные понятия и методы дискретной математики;
 - множества, функции и отношения, отношение эквивалентности, классы эквивалентности;
 - функции, инъекция, сюръекция, биекция, обратная функция, композиция функций, область определения и область значений, ядро;
 - основы теории графов;
 - элементы комбинаторики;
 - алгебраические структуры (группы, кольца, векторные пространства, поля);
 - теорию перечислений дискретных структур;
 - лемму Бернсайда и теорему Пойя;
 - дискретные методы кодирования и защиты компьютерной информации.
- Уметь
 - применять парадигмы, методы и средства формализованного описания действий исполнителя для решения поставленной задачи на практике,
 - кодировать числовые и символьные данные в двоичном виде и использовать эти знания для объяснения ошибок, которые могут возникнуть в процессе выполнения программ;
 - анализировать и представлять функции и отношения в дискретных моделях;
 - анализировать и определять тип конечных графов;
 - анализировать и выявлять тип комбинаторных конфигураций;
 - анализировать и определять тип абстрактной алгебры;
 - применять свои знания к решению практических задач;
 - пользоваться математической литературой для самостоятельного изучения моделей дискретной математики в программной инженерии.
- Иметь навыки
 - использования полученных знаний о процессах получения, преобразования, хранения, представления и использования информации в компьютере в различных контекстах;

- подготовки подробных отчетов о решении задач повышенной сложности при выполнении домашних заданий в первом, втором, третьем и четвертом модуле.

В результате освоения дисциплины студент осваивает следующие компетенции:

Компетенция	Код компетенции по ЕКК	Дескрипторы – основные признаки освоения (показатели достижения результата)	Формы и методы обучения, способствующие формированию и развитию компетенции
Способен учиться, приобретать новые знания, умения, в том числе в области, отличной от профессиональной	СК-Б1	<ul style="list-style-type: none"> - Проявляет навыки самостоятельного освоения материала - Знает определения основных понятий в том числе и на английском языке 	Лекции и практические занятия, повторение пройденного материала (консультации) и самостоятельная работа студентов (изучение теоретического материала, представленного в массовых открытых онлайн-курсах).
Способен применять основные концепции, принципы, теории и факты, связанные с информатикой при решении научно-исследовательских задач	ИК-1	<ul style="list-style-type: none"> - Умеет применять материал основных тем дисциплины при решении задач - Проявляет навыки логического и алгоритмического мышления в процессе решения тестовых задач по основным темам дисциплины 	Решение задач на практических занятиях, текущее и итоговое тестирование
Способен использовать методы и инструментальные средства исследования объектов профессиональной деятельности	ИК-3	<ul style="list-style-type: none"> - Проявляет навыки работы с инструментальными средствами при выполнении домашних заданий - Умеет оформлять отчеты по результатам выполнения домашнего задания 	Выполнение практических домашних заданий.

4 Место дисциплины в структуре образовательной программы

Настоящая дисциплина относится к базовой части Б.ПЦ.Б дисциплин профессионального цикла рабочего учебного плана направления 09.03.04 «Программная инженерия» подготовки бакалавра на 2017-2018 учебный год. Дисциплина читается студентам бакалаврской программы «Программная инженерия» факультета компьютерных наук НИУ ВШЭ. Она предлагается студентам в первом, втором, третьем и четвертом модулях первого года обучения. Продолжительность курса составляет **144** аудиторных учебных часов (в рамках 4 модулей), образованных **64** часа лекций и **80** часа практических занятий. Помимо этого, **160** часов в курсе отводится под самостоятельную работу студентов. Предусмотренный программой дисциплины текущий контроль включает: домашние задания (**Д** в первом, втором, третьем и четвертом модулях), контрольные работы (**К** в первом, втором, третьем и четвертом модулях), массовые открытые онлайн-курсы с использованием оригинальной англоязычной терминологии в первом и втором семестре (контроль освоения курсов **М** осуществляется в конце второго модуля и четвертого модуля). В конце первого и второго семестров проводится экзамен по дисциплине (**Э** в конце второго модуля и четвертого модулей).

Изучение данной дисциплины базируется на знаниях студентами математики, основ информатики и алгоритмизации в рамках учебной программы средней школы, умении применять математический аппарат при выборе метода решения поставленной задачи.

Основные положения дисциплины должны быть использованы в дальнейшем при изучении следующих дисциплин:

- Программирование (первый курс направления 09.03.04 «Программная инженерия»);

- Алгоритмы и структуры данных (второй курс направления 09.03.04 «Программная инженерия»);
- Конструирование программного обеспечения (второй курс направления 09.03.04 «Программная инженерия»);

5 Тематический план учебной дисциплины

№	Название темы	Всего часов по дисциплине	Аудиторные часы		Самостоятельная работа
			Лекции	Практические занятия	
Первый модуль. Лекций – 12 часов. Практических занятий – 16 часов. Самостоятельная работа – 36 часов. Формы текущего контроля – домашнее задание Д1, контрольная работа К1.					
1	Основные понятия математической логики. Высказывание. Логические связки. Силлогизм. Законы Аристотеля. Закон Лейбница. Логика высказываний. Пропозициональные переменные. Формулы логики высказываний. Равносильность формул. Тавтология. Противоречие. Выполнимость. Оправдываемость. Алгебра высказываний. Булева функция. Существенные и несущественные переменные. Таблицы истинности. Множество. Предикат. Свойство. Кванторы. Законы де Моргана.	8	1,5	2	4,5
2	Законы булевой алгебры. Абстрактные алгебры с одной и двумя операциями. Изоморфизмы алгебр. Классический принцип двойственности. Булева алгебра. Алгебра Кантора. Законы поглощения. Законы Порецкого. Законы склеивания. Компьютерное представление конечных множеств. Дизъюнктивное и конъюнктивное разложение Шеннона. Синтез логических формул. Предельные разложения Шеннона. Канонические формы. Совершенная дизъюнктивная нормальная форма СДНФ. Совершенная конъюнктивная нормальная форма СКНФ.	8	1,5	2	4,5
3	Дифференциальное исчисление булевых функций. Ортогональность. Разложения Рида. Полиномы Жегалкина. Логические уравнения. Теоретико-множественные уравнения. Побитовые уравнения. Система линейных алгебраических уравнений в поле Галуа GF(2). Производная. Дифференцирование булевых функций. Разложение булевой функции в ряд Тейлора и Маклорена. Алгебра переключательных схем. Комбинационные схемы и схемы с памятью. Методы решения логических задач.	8	1,5	2	4,5

4	Критерий Поста. Замкнутые классы логических функций. Полные системы булевых функций в сильном и слабом смысле. Базисы. Теорема Поста. Минимизация булевых функций в классе дизъюнктивных и конъюнктивных нормальных форм. Коды Грэя. Карты Карно. Частично-определенные функции и их минимизация. Минимизация булевых функций в заданных базисах.	8	1,5	2	4,5
5	Конечные автоматы. Автоматы Мили и Мура. Представление данных. Алфавит. Операция конкатенации. Транзитивное и рефлексивное замыкание Клини. Регулярные выражение и регулярные языки. Префиксные, суффиксные и инфиксные коды. Грамматики. Минимизация автоматов. Компьютер, как программно управляемый цифровой автомат.	8	1,5	2	4,5
6	Аксиоматическая теория высказываний. Язык и метаязык в логике высказываний. Аксиоматические системы. Системы аксиом. Правило вывода. Полнота, непротиворечивость и разрешимость формализованного исчисления высказываний. Независимость системы аксиом. Логическое следование. Принцип дедукции. Формальный вывод. Метод резолюций. Метод Вонга. Натуральное исчисление.	8	1,5	2	4,5
7	Формальные аксиоматические системы. Язык и метаязык, теоремы и метатеоремы формальной теории. Интерпретация и модели формальной теории. Синтаксис и семантика языка логики предикатов. Непротиворечивость формализованного исчисления предикатов. Теорема Геделя о неполноте. Клаузальная форма. Клаузальная логика. Семантика клаузальной формы. Инфиксная нотация. Семантические сети. Клаузы Хорна и их интерпретация. Метод резолюций в логике предикатов. Принцип логического программирования.	8	1,5	2	4,5
8	Неклассические логики. Интуиционистская логика. Конечнозначные логики. Нечеткая логика. Модальная логика. Типы модальностей. Модальные исчисления. Семантика Кripке. Временные (темперальные) логики. Алгоритмические логики.	8	1,5	2	4,5

<p style="text-align: center;">Второй модуль.</p> <p style="text-align: center;">Лекций – 12 часов. Практических занятий – 16 часов. Самостоятельная работа – 36 часов.</p> <p style="text-align: center;">Формы текущего контроля – домашнее задание Д2, контрольная работа К2,</p> <p style="text-align: center;">массовый открытый онлайн курс М12.</p> <p style="text-align: center;">Итоговый контроль – экзамен Э1.</p>
--

9	Формализация понятия алгоритма. Понятие алгоритма и вычислимой функции. Качественная и количественная теория алгоритмов. Понятие алгоритмической системы. Машина Тьюринга. Машина Поста. Тезис Тьюринга. Основная гипотеза теории алгоритмов в форме Тьюринга. Универсальная машина Тьюринга. Универсальная машина Поста.	8	1,5	2	4,5
10	Нормальный алгоритм Маркова. Основная гипотеза теории алгоритмов в форме Маркова. Эквивалентность определений алгоритма в виде машины Тьюринга и нормального алгоритма Маркова. Универсальный алгоритм Маркова.	8	1,5	2	4,5
11	Рекурсивные функции. Базовые функции. Операторы суперпозиции, примитивной рекурсии и минимизации. Примитивно рекурсивные функции. Частично-рекурсивные функции. Тезис Черча. Универсальная частично-рекурсивная функция. Эквивалентность формальных определений алгоритма. Алгоритмически неразрешимые задачи. Невычислимые функции.	8	1,5	2	4,5
12	Меры сложности алгоритмов. Понятие сложности алгоритмов и вычислений, эффективные алгоритмы. Легко и трудно разрешимые задачи. Полиномиальная эквивалентность. Недетерминированные алгоритмы. Недетерминированная машина Тьюринга. Классы задач P и NP. NP – полные и NP – трудные задачи. Квантовый компьютер и квантовые вычисления.	8	1,5	2	4,5
13	Основы теории информации. Кодирование информации. Блоковые коды. Префиксные коды. Командный код. Код Грея. Расстояние Хемминга. Коды, обнаруживающие ошибки. Коды, исправляющие ошибки. Код Хаффмана. Информационный объем сообщения. Формула Хартли. Информация, вероятность, энтропия. Формула Шеннона.	8	1,5	2	4,5
14	Системы счисления. Позиционные системы с натуральным основанием. Представление. Арифметические операции. Алгоритмы перевода чисел из одной системы счисления в другую. Смешанные системы счисления. Нетрадиционные системы счисления: симметричные и ассиметричные, уравновешенная троичная, с отрицательным основанием, негодвоичная, фибоначчиевая, факториальная, остаточных классов.	8	1,5	2	4,5

15	Форматы представления информации в компьютере. Стандарт IEEE 754-2008. Представление целых положительных, отрицательных и беззнаковых чисел. Прямой и дополнительный код. Представление вещественных чисел. Форматы для представления вещественных чисел со скрытой единицей. Представление текстовой информации. Представление графической информации. Представление звуковой информации. Методы сжатия информации.	8	1,5	2	4,5
16	Вычислительная погрешность. Приближенное представление вещественных чисел. Абсолютная и относительная погрешность. Погрешность выполнения арифметических операций. Аксиоматическое построение множества действительных чисел. Ошибки перевода вещественных чисел из десятичной системы в двоичную систему счисления. Ошибки представления. Ошибки округления. Ошибки сдвига и компенсации при выполнении арифметических операций.	8	1,5	2	4,5
Третий модуль.					
Лекций – 22 часа. Практических занятий – 22 часа. Самостоятельная работа – 44 часа.					
Формы текущего контроля – домашнее задание ДЗ, контрольная работа КЗ.					
17	Функции и отношения. Бинарные отношения и их свойства. Соответствия и функции. Изоморфизм и гомоморфизм отношений. Композиция отношений. Степень отношения. Ядро отношения. Отношение эквивалентности. Классы эквивалентности. Фактор множество. Отношения порядка. Замыкание отношений.	8,8	2	2,4	4,4
18	Основы теории графов. Графы, мультиграфы, псевдографы, орграфы. Изоморфизм графов. Способы задания графов. Операции над графиками. Маршруты, цепи, циклы. Ациклический граф. Топологическая сортировка. Расстояния между вершинами. Диаметр, радиус, центр графа.	8,8	2	2,4	4,4
19	Сильная и слабая связность. Компоненты связности. Точки сочленения. Вершинная и реберная связность. Мосты и блоки. Меры связности. Обходы графов. Циклы Эйлера, де Брёйна, Гамильтона.	8,8	2	2,4	4,4
20	Функциональные и контрафункциональные графы. Дерево и лес. Характеристические свойства деревьев. Каркасы (остовы) и хорды в связном графе. Ориентированные, упорядоченные, бинарные деревья. Алгоритмы обхода деревьев.	8,8	2	2,4	4,4

21	Фундаментальные системы циклов и разрезов (коциклов). Циклы в графах. Линейное пространство бинарных наборов. Линейное пространство подграфов данного графа. Подпространство четных подграфов. Циклический и коциклический ранг графа (цикломатическое и коцикломатическое число). Матричная теорема Киркгофа о деревьях. Алгоритм построения фундаментальной системы циклов в графе.	8,8	2	2,4	4,4
22	Алгоритмы на графах. Алгоритмы поиска в глубину и ширину. Взвешенные графы. Алгоритмы Крускала и Прима построения минимального остовного дерева. Алгоритмические задачи траекторного типа во взвешенном графе. Обобщенный алгоритм Дейкстры. Обобщенное уравнение Беллмана-Маслова. Обобщенный алгоритм Флойда-Уоршала.	8,8	2	2,4	4,4
23	Двудольные графы. Паросочетания. Алгоритм построения совершенного паросочетания для двудольного графа. Системы различных представителей для конечного семейства конечных множеств (трансверсаль). Теорема Холла о совершенных паросочетаниях.	8,8	2	2,4	4,4
24	Планарные графы. Укладка графа. Плоские графы. Эйлерова характеристика (формула Эйлера). Графы K_5 и $K_{3,3}$. Критерий планарности Понtryгина-Куратовского.	8,8	2	2,4	4,4
25	Раскраска графов. Хроматическое число и хроматический класс. Верхняя и нижняя оценка хроматического числа. Внутренне и внешне устойчивые множества вершин графа. Оптимальная раскраска вершин графа. Раскрашивание планарных графов. Теоремы о пяти и о четырех красках.	8,8	2	2,4	4,4
26	Потоки в сетях. Двухполюсные сети. Дивергенция. Разрезы (сечения). Величина потока и пропускная способность сети. Максимальный поток. Теорема Форда-Фалкерсона о максимальном потоке. Алгоритм построения максимального потока в сети. Многополюсная сеть. Обобщенная задача о назначениях и обобщенная транспортная задача. Алгоритмы решения обобщенной задачи о назначениях и обобщенной транспортной задачи.	8,8	2	2,4	4,4

Четвертый модуль.

Лекций – 20 часов. Практических занятий – 20 часов. Самостоятельная работа – 45 часов.
Формы текущего контроля – домашнее задание Д4, контрольная работа К4,
массовый открытый онлайн курс – М34.
Итоговый контроль – экзамен Э2.

27	Универсальные алгебры. Операция суперпозиции. Замыкания и подалгебры. Система образующих. Морфизмы, гомоморфизм и изоморфизм алгебр. Нарные отношения. Конгруэнции и фактор-алгебры. Группы, кольца, области целостности и поля. Векторные пространства. Решетки. Конечные группы, кольца и поля.	8,8	2	2,4	4,4
28	Матроиды. Базы и ранг матроида. Аксиоматические определения матроидов. Теорема о базах. Графовый матроид. Матроид Фано. Матроид паросочетаний. Матричный матроид. Жадный алгоритм. Теорема Радо-Эдмондса.	8,8	2	2,4	4,4
29	Сети Петри. Операционная семантика сетей Петри. Поведенческие свойства сетей Петри. Проблема достижимости и покрытие. Граф достижимости и деревья Карпа-Миллера. Живость и ограниченность. Инварианты позиций и переходов сетей Петри.	8,8	2	2,4	4,4
30	Модулярная арифметика. Делимость. Простые числа. Решето Эратосфена для нахождения простых чисел и неприводимых полиномов. Факторизация целых чисел. Метод выделения множителей Ферма. Наибольший общий делитель. Расширенный алгоритм Евклида. Наименьшее общее кратное. Функция Мебиуса и Эйлера. Теоремы Эйлера и Ферма.	8,8	2	2,4	4,4
31	Цепные и подходящие дроби. Алгоритм вычисления подходящих дробей. Решение линейных диофантовых уравнений. Полная и приведенная система вычетов. Решение сравнений. Китайская теорема об остатках.	8,8	2	2,4	4,4
32	Элементы теории кодирования. Алфавитное кодирование. Префиксный код. Кодирование с минимальной избыточностью. Алгоритмы Фано и Хаффмана. Хеммингово расстояние, Хемминговы сферы и корректирующая способность. Коды, обнаруживающие и исправляющие ошибки. Линейные блоковые коды. Порождающая и проверочная матрицы. Кодирование и декодирование линейных блоковых кодов. Коды Хэмминга. Двоичные циклические коды. Порождающий и проверочный полиномы.	8,8	2	2,4	4,4

33	Применение модулярной арифметики в криптографии. Симметричные и несимметричные криптосистемы. Криптографические протоколы. Криптография с открытым ключом. Шифросистемы и электронная цифровая подпись. Хэш-функция. Проблема квадратичного вычета. Проблема дискретного логарифма. Проблема подмножества суммы.	8,8	2	2,4	4,4
34	Проблема факторизации целых чисел. Проблема RSA. Факторизация полиномов над конечным полем. Крипто система RSA. Крипто система ЭльГамаля. Применение эллиптических кривых над конечными полями в криптографии. Обмен ключами по схеме Диффи-Хеллмана с использованием эллиптических кривых. Шифрование/дешифрование с использованием эллиптических кривых.	8,8	2	2,4	4,4
35	Элементы комбинаторики. Порождение комбинаторных конфигураций и их пересчет. Размещения, перестановки, сочетания без повторений и с повторениями. Подстановки, группа подстановок. Генерация перестановок. Биномиальные и полиномиальные коэффициенты, треугольник Паскаля, генерация подмножеств. Разбиения. Числа Стирлинга первого и второго рода, число Белла. Принцип включения и исключения. Производящие функции для комбинаторных конфигураций и их чисел. Аппарат формальных степенных рядов.	8,8	2	2,4	4,4
36	Числовые рекуррентные уравнения. Линейные рекуррентные уравнения (ЛРУ). Фундаментальная система решений. Общее решение ЛРУ с помощью фундаментальной системы решений. Стационарные ЛРУ (СЛРУ). Характеристический полином и характеристическое уравнение. Общее решение однородного и неоднородного СЛРУ. Частное решение неоднородного СЛРУ с правой частью – квазиполиномом.	8,8	2	2,4	4,4
	Итого:	304	64	80	160

6 Формы контроля знаний студентов

Тип контроля	Форма контроля	1 год				Параметры
		1 модуль	2 модуль	3 модуль	4 модуль	
Текущий (неделя)	Контрольные работы K1, K2, K3, K4	8 неделя	9 неделя	12 неделя	11 неделя	Компьютерное тестирование 20 тестовых заданий на 120 минут
	Домашние задания D1, D2, D3, D4	1-7 неделя	1-8 неделя	1-11 неделя	1-10 неделя	Использование инструментальных сред

	Массовые открытые онлайн- курсы M12, M34	1-8 неделя	1-8 неделя	1-11 неделя	1-10 неделя	Компьютерное тестиро- вание с использованием оригинальной англо- язычной терминологии
Итого- вый	Экзамен Э1, Э2		■		■	

6.1 Критерии оценки знаний, навыков

Текущий контроль в каждом модуле предусматривает домашнее задание и контрольную работу в виде теста на компьютере.

Элементы текущего контроля первого модуля:

Д1 – оценка за первое домашнее задание. Срок сдачи домашнего задания – седьмая неделя первого модуля. Оценка за домашнее задание выставляется по десятибалльной шкале при условии сдачи задания в срок и по восьмибалльной шкале в ином случае. Студенты, не сдавшие домашнее задание, получают оценку **Д1=0** баллов.

К1 – оценка за контрольную работу в первом модуле. Контрольная работа проводится в компьютерном классе по окончанию первого модуля в форме компьютерного тестирования. Студенты, не явившиеся на компьютерное тестирование, получают оценку **К1=0** баллов. Оценка за контрольную работу выставляется по десятибалльной шкале при условии выполнения контрольной работы в срок и по восьмибалльной шкале в ином случае.

Тематика тестовых заданий, предлагаемых студентам на контрольной работе, охватывает темы дисциплины, которые обсуждаются на лекционных и практических занятиях в первом модуле. В процессе выполнения контрольной работы студент должен продемонстрировать владение культурой мышления, способность к обобщению, анализу, восприятию информации, постановке цели и выбору путей её достижения, проявить навыки логического и алгоритмического мышления в процессе решения тестовых задач по основным темам дисциплины, понимать основные концепции, принципы, теории и факты, связанных с информатикой, знать определения основных понятий, уметь применять материал основных тем дисциплины при решении задач.

Количество включенных в работу тестовых заданий – 20. Продолжительность контрольной работы составляет 120 минут.

Элементы текущего контроля второго модуля:

Д2 – оценка за второе домашнее задание. Срок сдачи домашнего задания – восьмая неделя второго модуля. Оценка за домашнее задание выставляется по десятибалльной шкале при условии сдачи задания в срок и по восьмибалльной шкале в ином случае. Студенты, не сдавшие домашнее задание, получают оценку **Д2=0** баллов.

К2 – оценка за контрольную работу во втором модуле. Контрольная работа проводится в компьютерном классе по окончанию второго модуля в форме компьютерного тестирования. Студенты, не явившиеся на компьютерное тестирование, получают оценку **К2=0** баллов. Оценка за контрольную работу выставляется по десятибалльной шкале при условии выполнения контрольной работы в срок и по восьмибалльной шкале в ином случае.

Тематика тестовых заданий, предлагаемых студентам на контрольной работе, охватывает темы дисциплины, которые обсуждаются на лекционных и практических занятиях во втором модуле. В процессе выполнения контрольной работы студент должен продемонстрировать владение культурой мышления, способность к обобщению, анализу, восприятию информации, постановке цели и выбору путей её достижения, проявить навыки логического и алгоритмического мышления в процессе решения тестовых задач по основным темам дисциплины, понимать основные концепции, принципы, теории и факты, связанных с информатикой, знать определения основных понятий, уметь применять материал основных тем дисциплины при решении задач.

Количество, включенных в работу тестовых заданий – 20. Продолжительность контрольной работы составляет 120 минут.

M12 – оценка за прохождение семестрового массового открытого онлайн-курса (Coursera) «Введение в логику» (Introduction to Logic). Успешное прохождение курса «Введение в логику» демонстрирует владение англоязычной терминологией в рамках курса и способность к самостоятельному изучению материала на английском языке. Оценка определяется по результатам выполнения компьютерного теста на английском языке в конце 2 модуля. Студенты, не явившиеся на компьютерное тестирование, получают оценку **M12=0** баллов. Оценка за контрольную работу выставляется по десятибалльной шкале при условии выполнения компьютерного теста в срок и по восьмибалльной шкале в ином случае.

Тематика тестовых заданий, предлагаемых студентам в teste, охватывает темы курса «Введение в логику». В процессе выполнения тестирования студент должен продемонстрировать владение материалом курса, способность к обобщению, анализу, восприятию информации, постановке цели и выбору путей её достижения, проявить навыки логического и алгоритмического мышления в процессе решения тестовых задач, понимать основные концепции, принципы, теории и факты, связанных с материалом курса, знать определения основных понятий, уметь применять материал основных тем дисциплины при решении задач.

Количество, включенных в работу тестовых заданий – 20. Продолжительность теста составляет 120 минут.

Элементы текущего контроля третьего модуля:

D3 – оценка за третье домашнее задание. Срок сдачи домашнего задания – одиннадцатая неделя третьего модуля. Оценка за домашнее задание выставляется по десятибалльной шкале при условии сдачи задания в срок и по восьмибалльной шкале в ином случае. Студенты, не сдавшие домашнее задание, получают оценку **D3=0** баллов.

K3 – оценка за контрольную работу в третьем модуле. Контрольная работа проводится в компьютерном классе по окончанию третьего модуля в форме компьютерного тестирования. Студенты, не явившиеся на компьютерное тестирование, получают оценку **K3=0** баллов. Оценка за контрольную работу выставляется по десятибалльной шкале при условии выполнения контрольной работы в срок и по восьмибалльной шкале в ином случае.

Тематика тестовых заданий, предлагаемых студентам на контрольной работе, охватывает темы дисциплины, которые обсуждаются на лекционных и практических занятиях в третьем модуле. В процессе выполнения контрольной работы студент должен продемонстрировать владение культурой мышления, способность к обобщению, анализу, восприятию информации, постановке цели и выбору путей её достижения, проявить навыки логического и алгоритмического мышления в процессе решения тестовых задач по основным темам дисциплины, понимать основные концепции, принципы, теории и факты, связанных с информатикой, знать определения основных понятий, уметь применять материал основных тем дисциплины при решении задач.

Количество включенных в работу тестовых заданий – 20. Продолжительность контрольной работы составляет 120 минут.

Элементы текущего контроля четвертого модуля:

D4 – оценка за второе домашнее задание. Срок сдачи домашнего задания – десятая неделя второго модуля. Оценка за домашнее задание выставляется по десятибалльной шкале при условии сдачи задания в срок и по восьмибалльной шкале в ином случае. Студенты, не сдавшие домашнее задание, получают оценку **D4=0** баллов.

K4 – оценка за контрольную работу во втором модуле. Контрольная работа проводится в компьютерном классе по окончанию четвертого модуля в форме компьютерного тестирования. Студенты, не явившиеся на компьютерное тестирование, получают оценку **K4=0** баллов. Оценка за контрольную работу выставляется по десятибалльной шкале при условии выполнения контрольной работы в срок и по восьмибалльной шкале в ином случае.

Тематика тестовых заданий, предлагаемых студентам на контрольной работе, охватывает темы дисциплины, которые обсуждаются на лекционных и практических занятиях во четвертом модуле. В процессе выполнения контрольной работы студент должен продемонстрировать владение культурой мышления, способность к обобщению, анализу, восприятию информации, постановке цели и выбору путей её достижения, проявить навыки логического и алгоритмического мышления в процессе решения тестовых задач по основным темам дисциплины, понимать основные концепции, принципы, теории и факты, связанных с информатикой, знать определения основных понятий, уметь применять материал основных тем дисциплины при решении задач.

Количество, включенных в работу тестовых заданий – 20. Продолжительность контрольной работы составляет 120 минут.

M34 – оценка за прохождение семестрового открытого курса (MIT OpenCourseware) «Математика для компьютерных наук» (Mathematics for Computer Science, 6.042J / 18.062J). Успешное прохождение курса «Математика для компьютерных наук» демонстрирует владение англоязычной терминологией в рамках курса и способность к самостоятельному изучению материала на английском языке. Оценка определяется по результатам выполнения компьютерного теста на английском языке в конце 4 модуля. Студенты, не явившиеся на компьютерное тестирование, получают оценку **M34=0** баллов. Оценка за контрольную работу выставляется по десятибалльной шкале при условии выполнения компьютерного теста в срок и по восьмибалльной шкале в ином случае.

Тематика тестовых заданий, предлагаемых студентам в teste, охватывает темы курса «Математика для компьютерных наук». В процессе выполнения тестирования студент должен продемонстрировать владение материалом курса, способность к обобщению, анализу, восприятию информации, постановке цели и выбору путей её достижения, проявить навыки логического и алгоритмического мышления в процессе решения тестовых задач, понимать основные концепции, принципы, теории и факты, связанных с материалом курса, знать определения основных понятий, уметь применять материал основных тем дисциплины при решении задач.

Количество, включенных в работу тестовых заданий – 20. Продолжительность теста составляет 120 минут.

6.2 Порядок формирования оценок по дисциплине

На текущую оценку по учебной дисциплине в первом семестре влияют следующие элементы текущего контроля:

Д1 – оценка за домашнее задание в первом модуле.

Д2 – оценка за домашнее задание во втором модуле.

К1 – оценка за контрольную работу в первом модуле.

К2 – оценка за контрольную работу во втором модуле.

М12 – оценка за прохождение семестрового массового открытого онлайн-курса «Введение в логику» в первом семестре.

Оценка за текущий контроль по дисциплине **O1** в первом семестре учитывает результаты работы студента в модулях и формируется по десятибалльной шкале как взвешенная сумма полученных оценок текущего контроля по формулам:

$$D12 = (D1 < D2) ? (0.62*D1 + 0.38*D2) : (0.38*D1 + 0.62*D2)$$

$$K12 = (K1 < K2) ? (0.62*K1 + 0.38*K2) : (0.38*K1 + 0.62*K2)$$

$$O1 = (D12 < K12) ? (0.62*D12 + 0.38*K12) : (0.38*D12 + 0.62*K12)$$

с учетом правил округления до целого числа баллов.

Итоговая оценка за первый семестр **Э1** вычисляется по формуле:

$$E1 = 0.8*O1 + 0.2*M12$$

с учетом правил округления до целого числа баллов.

В случае если итоговая оценка за первый семестр **Э1 < 4**, студенту предлагается выполнить итоговое экзаменационное задание, состоящее из компьютерных тестирований **K12** и **M12** и двух творческих заданий **T1** и **T2**, каждое из которых оценивается по десятибалльной шкале.

Тематика тестовых заданий, предлагаемых студентам на экзамене, охватывает темы дисциплины, которые обсуждаются на лекционных и практических занятиях в первом и втором модуле и в рамках массового открытого онлайн-курса. В процессе выполнения экзаменационного задания студент должен продемонстрировать владение культурой мышления, способность к обобщению, анализу, восприятию информации, постановке цели и выбору путей её достижения, проявить навыки логического и алгоритмического мышления в процессе решения тестовых задач по основным темам дисциплины, понимать основные концепции, принципы, теории и факты, связанных с информатикой, знать определения основных понятий, уметь применять материал основных тем дисциплины при решении задач.

Количество включенных в каждый из тестов **K12** и **M12** тестовых заданий – 20. Продолжительность каждого из тестов составляет 120 минут. Набор тестовых заданий теста **K12** представляет собой подмножество тестовых заданий первой и второй контрольной работы.

Первое творческое задание **T1** формулируется по материалам, изученным в первом модуле и соответствует по тематике первому домашнему заданию, второе творческое задание **T2** формулируется по материалам, изученным во втором модуле и соответствует по тематике второму домашнему заданию. На выполнение двух творческих заданий отводится 120 минут.

Итоговая оценка за первый семестр **Э1** в этом случае вычисляется по формулам:

$$T12 = (T1 < T2) ? (0.62*T1 + 0.38*T2) : (0.38*T1 + 0.62*T2)$$

$$E1 = 0.8*((T12 < K12) ? (0.62*T12 + 0.38*K12) : (0.38*T12 + 0.62*K12)) + 0.2*M12$$

с учетом правил округления до целого числа баллов. Здесь:

T1 - оценка за первое творческое задание,

T2 - оценка за второе творческое задание,

K12 - оценка за выполнение тестовых заданий в компьютерной форме,

M12 – оценка за выполнение компьютерного теста на английском языке по материалам семестрового массового открытого онлайн-курса «Введение в логику».

При пересдаче итогового экзамена за первый семестр (независимо от предыдущих оценок) итоговая экзаменационная оценка **Э1** по дисциплине формируется как взвешенная сумма полученных оценок, по формулам:

$$T12 = (T1 < T2) ? (0.62*T1 + 0.38*T2) : (0.38*T1 + 0.62*T2)$$

$$\mathcal{E}1 = 0.8*((T12 < K12) ? (0.62*T12 + 0.38*K12) : (0.38*T12 + 0.62*K12)) + 0.2*M12$$

с учетом правил округления до целого числа баллов.

Правила округления до целого числа баллов при выставлении оценок: средневзвешенная оценка округляется до большего целого, если дробная часть оценки не ниже 0,5, в противном случае оценка округляется до меньшего целого.

Во втором семестре оценка за текущий контроль по дисциплине О2 и итоговая оценка за второй семестр Э2 формируются аналогично.

На текущую оценку по учебной дисциплине во втором семестре влияют следующие элементы текущего контроля:

Д3 – оценка за домашнее задание в третьем модуле.

Д4 – оценка за домашнее задание в четвертом модуле.

K3 – оценка за контрольную работу в третьем модуле.

K4 – оценка за контрольную работу в четвертом модуле.

M34 – оценка за прохождение семестрового массового открытого онлайн-курса «Математика для компьютерных наук» во втором семестре.

Оценка за текущий контроль по дисциплине **О2** во втором семестре учитывает результаты работы студента в модулях и формируется по десятибалльной шкале как взвешенная сумма полученных оценок текущего контроля по формулам:

$$D34 = (D3 < D4) ? (0.62*D3 + 0.38*D4) : (0.38*D3 + 0.62*D4)$$

$$K34 = (K3 < K4) ? (0.62*K3 + 0.38*K4) : (0.38*K3 + 0.62*K4)$$

$$O2 = (D34 < K34) ? (0.62*D34 + 0.38*K34) : (0.38*D34 + 0.62*K34)$$

с учетом правил округления до целого числа баллов.

Итоговая оценка за второй семестр Э2 вычисляется по формуле:

$$E2 = 0.8*O2 + 0.2*M34$$

с учетом правил округления до целого числа баллов.

В случае если итоговая оценка за первый семестр **Э2 < 4**, студенту предлагается выполнить итоговое экзаменационное задание, состоящее из компьютерных тестирований **K34** и **M34** и двух творческих заданий **T3** и **T4**, каждое из которых оценивается по десятибалльной шкале.

Тематика тестовых заданий, предлагаемых студентам на экзамене, охватывает темы дисциплины, которые обсуждаются на лекционных и практических занятиях в первом и втором модуле и в рамках массового открытого онлайн-курса. В процессе выполнения экзаменационного задания студент должен продемонстрировать владение культурой мышления, способность к обобщению, анализу, восприятию информации, постановке цели и выбору путей её достижения, проявить

навыки логического и алгоритмического мышления в процессе решения тестовых задач по основным темам дисциплины, понимать основные концепции, принципы, теории и факты, связанных с информатикой, знать определения основных понятий, уметь применять материал основных тем дисциплины при решении задач.

Количество включенных в каждый из тестов **K34** и **M34** тестовых заданий – 20. Продолжительность каждого из тестов составляет 120 минут. Набор тестовых заданий теста **K12** представляет собой подмножество тестовых заданий третьей и четвертой контрольной работы.

Третье творческое задание **T3** формулируется по материалам, изученным в третьем модуле и соответствует по тематике третьему домашнему заданию, четвертое творческое задание **T4** формулируется по материалам, изученным в четвертом модуле и соответствует по тематике четвертому домашнему заданию. На выполнение двух творческих заданий отводится 120 минут.

Итоговая оценка за второй семестр Э2 в этом случае вычисляется по формулам:

$$T34 = (T3 < T4) ? (0.62*T3 + 0.38*T4) : (0.38*T3 + 0.62*T4)$$

$$\mathcal{E}2 = 0.8*((T34 < K34) ? (0.62*T34 + 0.38*K34) : (0.38*T34 + 0.62*K34)) + 0.2*M34$$

с учетом правил округления до целого числа баллов. Здесь:

T3 - оценка за третье творческое задание,

T4 - оценка за четвертое творческое задание,

K34 - оценка за выполнение тестовых заданий в компьютерной форме,

M34 – оценка за выполнение компьютерного теста на английском языке по материалам семестрового массового открытого онлайн-курса «Математика для компьютерных наук».

При пересдаче итогового экзамена за второй семестр (независимо от предыдущих оценок) итоговая экзаменационная оценка **Э2** по дисциплине формируется как взвешенная сумма полученных оценок, по формулам:

$$T34 = (T3 < T4) ? (0.62*T3 + 0.38*T4) : (0.38*T3 + 0.62*T4)$$

$$\mathcal{E}2 = 0.8*((T34 < K34) ? (0.62*T34 + 0.38*K34) : (0.38*T34 + 0.62*K34)) + 0.2*M34$$

с учетом правил округления до целого числа баллов.

Правила округления до целого числа баллов при выставлении оценок: средневзвешенная оценка округляется до большего целого, если дробная часть оценки не ниже 0,5, в противном случае оценка округляется до меньшего целого.

Результирующая оценка Р по дисциплине формируется по десятибалльной шкале как взвешенная сумма полученных оценок итогового контроля первого и второго семестров с учетом правил округления до целого числа баллов по следующей формуле

$$P = ((\mathcal{E}1 > 3) \& (\mathcal{E}2 > 3)) ? (0.5*\mathcal{E}1 + 0.5*\mathcal{E}2) : (\mathcal{E}1 < \mathcal{E}2) ? \mathcal{E}1 : \mathcal{E}2$$

Правила округления до целого числа баллов при выставлении оценок: средневзвешенная оценка округляется до большего целого, если дробная часть оценки не ниже 0,5, в противном случае оценка округляется до меньшего целого.

Перевод экзаменационных оценок **Э1**, **Э2** и результирующей оценки **P** по дисциплине в оценку по пятибалльной шкале осуществляется в соответствии со следующей таблицей:

Таблица соответствия оценок по десятибалльной и пятибалльной системам

По десятибалльной шкале	По пятибалльной шкале
1 – неудовлетворительно 2 – очень плохо 3 – плохо	неудовлетворительно – 2

По десятибалльной шкале	По пятибалльной шкале
4 – удовлетворительно 5 – весьма удовлетворительно	удовлетворительно – 3
6 – хорошо 7 – очень хорошо	хорошо – 4
8 – почти отлично 9 – отлично 10 – блестяще	отлично – 5

7 Содержание дисциплины

◆ Тема 1. Основные понятия математической логики.

Содержание лекционных занятий.

Высказывание. Логические связки. Силлогизм. Законы Аристотеля. Закон Лейбница. Логика высказываний. Пропозициональные переменные. Формулы логики высказываний. Равносильность формул. Тавтология. Противоречие. Выполнимость. Опровергимость. Алгебра высказываний. Булева функция. Существенные и несущественные переменные. Таблицы истинности. Множество. Предикат. Свойство. Кванторы. Законы де Моргана.

Содержание практических занятий.

Построение таблиц истинности логических формул. Разбиение заданных логических формул на тавтологии и опровергимые формулы, на противоречия и выполнимые формулы. Определение существенных и несущественных переменных. Решение задач на применение законов де Моргана.

Основная литература:

- **Андерсон Дж.** Дискретная математика и комбинаторика. М.: Вильямс, 2004. – 960 с.
- **Колмогоров А.Н., Драгалин А.Г.** Математическая логика. Введение в математическую логику. Едиториал УРСС, 2013. – 240.
- **Новиков Ф.А.** Дискретная математика для программистов. СПб.: Питер, 2008. – 384 с.
- **Хаггарти Р.** Дискретная математика для программистов. Техносфера, 2012. – 400 с.

Дополнительная литература:

- **Rosen K.H.** Discrete Mathematics and Its Applications. – 7th edition. McGraw-Hill, 2012. – 1071 p.
- **Верещагин Н.К., Шень А.** Начала теории множеств. МЦНМО, 2012. – 112 с.
- **Гринченков Д.В., Потоцкий С.И.** Математическая логика и теория алгоритмов для программистов. М.: КноРус, 2012. – 206 с.
- **Гуц А.К.** Математическая логика и теория алгоритмов. Либерком, 2009. – 120 с.
- **Клини С.К.** Введение в метаматематику. М.: Либроком, 2008. – 526 с.
- **Клини С.К.** Математическая логика. М.: ЛКИ, 2008. – 482 с.
- **Лавров И.А.** Математическая логика. М.: Академия, 2006. – 240 с.
- **Лавров И.А., Максимова Л.Л.** Задачи по теории множеств, математической логике и теории алгоритмов. М.: Физматлит, 2004. – 256 с.
- **Ландо С.К.** Введение в дискретную математику. МЦНМО, 2012. – 272 с.
- **Локшин А.А., Сагомонян Е.А.** Логика и множества. М.: “Вузовская книга”, 2002. – 64 с.
- **Мендельсон Э.** Введение в математическую логику. М.: Либроком, 2010. – 161 с.
- **Набебин А.А., Кораблин Ю.П.** Математическая логика и теория алгоритмов. Научный мир, 2008. – 344 с.
- **Непейвода Н.Н.** Прикладная логика. – Новосибирск, НГУ, 2000. - 494 с.
- **Черч А.** Введение в математическую логику. Том 1. Либроком, 2009. – 482 с.

- **Хаггарти Р., Шлипф Дж., Уайтсайдс С.** Дискретная математика для программистов. Бином, Лаборатория знаний, 2010. – 632 с.
- **Яблонский С.В.** Введение в дискретную математику. Высшая школа. 2012. – 384 с.

◆ **Тема 2. Законы булевой алгебры.**

Содержание лекционных занятий.

Абстрактные алгебры с одной и двумя операциями. Изоморфизмы алгебр. Классический принцип двойственности. Булева алгебра. Алгебра Кантора. Законы поглощения. Законы Порецкого. Законы склеивания. Компьютерное представление конечных множеств. Дизъюнктивное и конъюнктивное разложение Шеннона. Синтез логических формул. Предельные разложения Шеннона. Канонические формы. Совершенная дизъюнктивная нормальная форма СДНФ. Совершенная конъюнктивная нормальная форма СКНФ.

Содержание практических занятий.

Построение пар двойственных логических функций, заданных таблицами истинности. Решение задач на определение свойств пар двойственных логических бинарных операций. Решение задач на применение законов булевой алгебры, алгебры Кантора, классического принципа двойственности и разложения функций в канонические формы.

Основная литература:

- **Андерсон Дж.** Дискретная математика и комбинаторика. М.: Вильямс, 2004. – 960 с.
- **Колмогоров А.Н., Драгалин А.Г.** Математическая логика. Введение в математическую логику. Едиториал УРСС, 2013. – 240.

Дополнительная литература:

- **Rosen K.H.** Discrete Mathematics and Its Applications. – 7th edition. McGraw-Hill, 2012. – 1071 p.
- **Верещагин Н.К., Шень А.** Начала теории множеств. МЦНМО, 2012. – 112 с.
- **Гринченков Д.В., Потоцкий С.И.** Математическая логика и теория алгоритмов для программистов. М.: КноРус, 2012. – 206 с.
- **Гуц А.К.** Математическая логика и теория алгоритмов. Либерком, 2009. – 120 с.
- **Клини С.К.** Введение в метаматематику. М.: Либроком, 2008. – 526 с.
- **Клини С.К.** Математическая логика. М.: ЛКИ, 2008. – 482 с.
- **Лавров И.А.** Математическая логика. М.: Академия, 2006. – 240 с.
- **Лавров И.А., Максимова Л.Л.** Задачи по теории множеств, математической логике и теории алгоритмов. М.: Физматлит, 2004. – 256 с.
- **Ландо С.К.** Введение в дискретную математику. МЦНМО, 2012. – 272 с.
- **Локшин А.А., Сагомонян Е.А.** Логика и множества. М.: “Вузовская книга”, 2002. – 64 с.
- **Мендельсон Э.** Введение в математическую логику. М.: Либроком, 2010. – 161 с.
- **Набебин А.А., Кораблин Ю.П.** Математическая логика и теория алгоритмов. Научный мир, 2008. – 344 с.
- **Непейвода Н.Н.** Прикладная логика. – Новосибирск, НГУ, 2000. - 494 с.
- **Черч А.** Введение в математическую логику. Том 1. Либроком, 2009. – 482 с.
- **Хаггарти Р., Шлипф Дж., Уайтсайдс С.** Дискретная математика для программистов. Бином, Лаборатория знаний, 2010. – 632 с.
- **Яблонский С.В.** Введение в дискретную математику. Высшая школа. 2012. – 384 с.

◆ **Тема 3. Дифференциальное исчисление булевых функций.**

Содержание лекционных занятий.

Ортогональность. Разложения Рида. Полиномы Жегалкина. Логические уравнения. Теоретико-множественные уравнения. Побитовые уравнения. Система линейных алгебраических

уравнений в поле Галуа GF(2). Производная. Дифференцирование булевых функций. Разложение булевой функции в ряд Тейлора и Маклорена. Алгебра переключательных схем. Комбинационные схемы и схемы с памятью. Методы решения логических задач.

Содержание практических занятий.

Разложение функций в ряды. Алгоритмы решения систем линейных уравнений в полях Галуа. Решение логических и теоретико-множественных уравнений. Определение функций, реализуемых переключательными и комбинационными схемами. Построение переключательных и комбинационных схем, реализующих заданную функцию. Решение логических задач.

Основная литература:

- **Андерсон Дж.** Дискретная математика и комбинаторика. М.: Вильямс, 2004. – 960 с.
- **Колмогоров А.Н., Драгалин А.Г.** Математическая логика. Введение в математическую логику. Едиториал УРСС, 2013. – 240.
- **Кузнецов О.П.** Дискретная математика для инженеров. М.: Лань, 2005. – 400 с.

Дополнительная литература:

- **Непейвода Н.Н.** Прикладная логика. – Новосибирск, НГУ, 2000. - 494 с.
- **Смолин Ю.Н.** Числовые системы. Флинта, Наука. -2009. – 112 с.

◆ Тема 4. Критерий Поста.

Содержание лекционных занятий.

Замкнутые классы логических функций. Полные системы булевых функций в сильном и слабом смысле. Базисы. Теорема Поста. Минимизация булевых функций в классе дизъюнктивных и конъюнктивных нормальных форм. Коды Грея. Карты Карно. Частично-определенные функции и их минимизация. Минимизация булевых функций в заданных базисах.

Содержание практических занятий.

Определение заданной булевой функции к замкнутым классам. Выражение логических функций в заданных базисах. Решение задач на минимизацию частично-определенных и всюду определенных функций в заданных базисах.

Основная литература:

- **Андерсон Дж.** Дискретная математика и комбинаторика. М.: Вильямс, 2004. – 960 с.
- **Кузнецов О.П.** Дискретная математика для инженеров. М.: Лань, 2005. – 400 с.
- **Набебин А.А.** Дискретная математика. Научный мир, 2010. – 512 с.
- **Новиков Ф.А.** Дискретная математика для программистов. СПб.: Питер, 2008. – 384 с.

Дополнительная литература:

- **Набебин А.А.** Сборник заданий по дискретной математике. Научный мир, 2009. – 280 с.
- **Новиков Ф.А.** Дискретная математика. Питер, 2012. – 400 с.

◆ Тема 5. Конечные автоматы.

Содержание лекционных занятий.

Автоматы Мили и Мура. Представление данных. Алфавит. Операция конкатенации. Транзитивное и рефлексивное замыкание Клини. Регулярные выражение и регулярные языки. Префиксные, суффиксные и инфиксные коды. Грамматики. Минимизация автоматов. Компьютер, как программируемый цифровой автомат.

Содержание практических занятий.

Построение автоматов, реализующих заданное преобразование. Схемы с памятью, построенные на основе логических функций. Триггер. Регистр. Сумматор. Шифратор и дешифратор. Построение автоматов, распознающих регулярные языки. Алгоритмы минимизации автоматов Мили и Мура.

Основная литература:

- **Андерсон Дж.** Дискретная математика и комбинаторика. М.: Вильямс, 2004. – 960 с.
- **Кузнецов О.П.** Дискретная математика для инженеров. М.: Лань, 2005. – 400 с.
- **Хаггарти Р.** Дискретная математика для программистов. Техносфера, 2012. – 400 с.

Дополнительная литература:

- **Хаггарти Р., Шлипф Дж., Уайтсайд С.** Дискретная математика для программистов. Бином, Лаборатория знаний, 2010. – 632 с.

◆ Тема 6. Аксиоматическая теория высказываний.

Содержание лекционных занятий.

Язык и метаязык в логике высказываний. Аксиоматические системы. Системы аксиом. Правило вывода. Полнота, непротиворечивость и разрешимость формализованного исчисления высказываний. Независимость системы аксиом. Логическое следование. Принцип дедукции. Формальный вывод. Метод резолюций. Метод Вонга. Натуральное исчисление.

Содержание практических занятий.

Решение задач на доказательство на основе аксиоматического метода, метода натурального исчисления, метода резолюций и метода Вонга.

Основная литература:

- **Андерсон Дж.** Дискретная математика и комбинаторика. М.: Вильямс, 2004. – 960 с.
- **Колмогоров А.Н., Драгалин А.Г.** Математическая логика. Введение в математическую логику. Едиториал УРСС, 2013. – 240.

Дополнительная литература:

- **Верещагин Н.К., Шень А.** Языки и исчисления. МЦНМО, 2012. – 240 с.
- **Гуц А.К.** Математическая логика и теория алгоритмов. Либерком, 2009. – 120 с.
- **Клини С.К.** Введение в метаматематику. М.: Либроком, 2008. – 526 с.
- **Клини С.К.** Математическая логика. М.: ЛКИ, 2008. – 482 с.
- **Лавров И.А.** Математическая логика. М.: Академия, 2006. – 240 с.
- **Лавров И.А., Максимова Л.Л.** Задачи по теории множеств, математической логике и теории алгоритмов. М.: Физматлит, 2004. – 256 с.
- **Локшин А.А., Сагомонян Е.А.** Логика и множества. М.: “Вузовская книга”, 2002. – 64 с.
- **Мендельсон Э.** Введение в математическую логику. М.: Либроком, 2010. – 161 с.
- **Непейвода Н.Н.** Прикладная логика. – Новосибирск, НГУ, 2000. - 494 с.
- **Черч А.** Введение в математическую логику. Том 1. Либроком, 2009. – 482 с.

◆ Тема 7. Формальные аксиоматические системы.

Содержание лекционных занятий.

Язык и метаязык, теоремы и метатеоремы формальной теории. Интерпретация и модели формальной теории. Синтаксис и семантика языка логики предикатов. Непротиворечивость формализованного исчисления предикатов. Теорема Геделя о неполноте. Клаузуальная форма. Клаузуальная логика. Семантика клаузуальной формы. Инфиксная нотация. Семантические сети. Клаузы Хорна и их интерпретация. Метод резолюций в логике предикатов. Принцип логического программирования.

Содержание практических занятий.

Решение задач на доказательство в логике предикатов. Алгоритмы процедур унификации и резолюций в Прологе. Трассировка алгоритмов на языке Пролог. Решение задач на основе семантических сетей.

Основная литература:

- **Андерсон Дж.** Дискретная математика и комбинаторика. М.: Вильямс, 2004. – 960 с.
- **Колмогоров А.Н., Драгалин А.Г.** Математическая логика. Введение в математическую логику. Едиториал УРСС, 2013. – 240.

Дополнительная литература:

- **Верещагин Н.К., Шень А.** Языки и исчисления. МЦНМО, 2012. – 240 с.
- **Гуц А.К.** Математическая логика и теория алгоритмов. Либерком, 2009. – 120 с.
- **Клини С.К.** Введение в метаматематику. М.: Либроком, 2008. – 526 с.
- **Клини С.К.** Математическая логика. М.: ЛКИ, 2008. – 482 с.
- **Лавров И.А.** Математическая логика. М.: Академия, 2006. – 240 с.
- **Лавров И.А., Максимова Л.Л.** Задачи по теории множеств, математической логике и теории алгоритмов. М.: Физматлит, 2004. – 256 с.
- **Мендельсон Э.** Введение в математическую логику. М.: Либроком, 2010. – 161 с.
- **Непейвода Н.Н.** Прикладная логика. – Новосибирск, НГУ, 2000. - 494 с.
- **Черч А.** Введение в математическую логику. Том 1. Либроком, 2009. – 482 с.

◆ Тема 8. Неклассические логики.

Содержание лекционных занятий.

Интуиционистская логика. Конечнозначные логики. Нечеткая логика. Модальная логика. Типы модальностей. Модальные исчисления. Семантика Крипке. Временные (tempоральные) логики. Алгоритмические логики.

Содержание практических занятий.

Решение задач с использованием конечнозначных и нечетких логик.

Основная литература:

- **Андерсон Дж.** Дискретная математика и комбинаторика. М.: Вильямс, 2004. – 960 с.
- **Колмогоров А.Н., Драгалин А.Г.** Математическая логика. Введение в математическую логику. Едиториал УРСС, 2013. – 240.

Дополнительная литература:

- **Гуц А.К.** Математическая логика и теория алгоритмов. Либерком, 2009. – 120 с.
- **Клини С.К.** Введение в метаматематику. М.: Либроком, 2008. – 526 с.
- **Клини С.К.** Математическая логика. М.: ЛКИ, 2008. – 482 с.
- **Лавров И.А.** Математическая логика. М.: Академия, 2006. – 240 с.
- **Лавров И.А., Максимова Л.Л.** Задачи по теории множеств, математической логике и теории алгоритмов. М.: Физматлит, 2004. – 256 с.
- **Мендельсон Э.** Введение в математическую логику. М.: Либроком, 2010. – 161 с.
- **Черч А.** Введение в математическую логику. Том 1. Либроком, 2009. – 482 с.

◆ Тема 9. Формализация понятия алгоритма.

Содержание лекционных занятий.

Понятие алгоритма и вычислимой функции. Качественная и количественная теория алгоритмов. Понятие алгоритмической системы. Машина Тьюринга. Машина Поста. Тезис Тьюринга. Основная гипотеза теории алгоритмов в форме Тьюринга. Универсальная машина Тьюринга. Универсальная машина Поста.

Содержание практических занятий.

Решение задач на представление алгоритма в виде машины Тьюринга. Трассировка программ для машины Тьюринга. R-технология.

Основная литература:

- **Андерсон Дж.** Дискретная математика и комбинаторика. М.: Вильямс, 2004. – 960 с.

- **Андреева Е.В., Босова Л.Л., Фалина И.Н.** Математические основы информатики. М.: Бином, 2007. – 328 с.
- **Новиков Ф.А.** Дискретная математика для программистов. СПб.: Питер, 2008. – 384 с.
- **Хаггарти Р.** Дискретная математика для программистов. Техносфера, 2012. – 400 с.

Дополнительная литература:

- **Босс В.** Лекции по математике. Т. 6: Алгоритмы, логика, вычислимость. От Диофанта до Тьюринга и Геделя. Либроком, УРСС, 2012. – 2008 с.
- **Верещагин Н.К., Шень А.** Вычислимые функции. МЦНМО, 2012. – 160 с.
- **Гринченков Д.В., Потоцкий С.И.** Математическая логика и теория алгоритмов для программистов. М.: КноРус, 2012. – 206 с.
- **Гуц А.К.** Математическая логика и теория алгоритмов. Либерком, 2009. – 120 с.
- **Лавров И.А., Максимова Л.Л.** Задачи по теории множеств, математической логике и теории алгоритмов. М.: Физматлит, 2004. – 256 с.
- **Набебин А.А., Кораблин Ю.П.** Математическая логика и теория алгоритмов. Научный мир, 2008. – 344 с.
- **Хаггарти Р., Шлипф Дж., Уайтрайдс С.** Дискретная математика для программистов. Бином, Лаборатория знаний, 2010. – 632 с.

◆ Тема 10. Нормальный алгоритм Маркова.

Содержание лекционных занятий.

Основная гипотеза теории алгоритмов в форме Маркова. Эквивалентность определений алгоритма в виде машины Тьюринга и нормального алгоритма Маркова. Универсальный алгоритм Маркова.

Содержание практических занятий.

Решение задач на представление алгоритма в виде нормального алгоритма Маркова. Трасировка нормальных алгоритмов Маркова. Представление машин Тьюринга в виде нормального алгоритма Маркова.

Основная литература:

- **Андерсон Дж.** Дискретная математика и комбинаторика. М.: Вильямс, 2004. – 960 с.
- **Андреева Е.В., Босова Л.Л., Фалина И.Н.** Математические основы информатики. М.: Бином, 2007. – 328 с.

Дополнительная литература:

- **Босс В.** Лекции по математике. Т. 6: Алгоритмы, логика, вычислимость. От Диофанта до Тьюринга и Геделя. Либроком, УРСС, 2012. – 2008 с.
- **Верещагин Н.К., Шень А.** Вычислимые функции. МЦНМО, 2012. – 160 с.
- **Гринченков Д.В., Потоцкий С.И.** Математическая логика и теория алгоритмов для программистов. М.: КноРус, 2012. – 206 с.
- **Гуц А.К.** Математическая логика и теория алгоритмов. Либерком, 2009. – 120 с.

◆ Тема 11. Рекурсивные функции.

Содержание лекционных занятий.

Базовые функции. Операторы суперпозиции, примитивной рекурсии и минимизации. Примитивно рекурсивные функции. Частично-рекурсивные функции. Тезис Черча. Универсальная частично-рекурсивная функция. Эквивалентность формальных определений алгоритма. Алгоритмически неразрешимые задачи. Невычислимые функции.

Содержание практических занятий.

Решение задач на представление алгоритма в виде рекурсивной функции. Трассировка вычисления рекурсивных функций. Доказательство алгоритмической неразрешимости ряда задач о самоприменимости, остановки, самоаннулируемости, анулируемости и т.д,

Основная литература:

- **Андерсон Дж.** Дискретная математика и комбинаторика. М.: Вильямс, 2004. – 960 с.
- **Хаггарти Р.** Дискретная математика для программистов. Техносфера, 2012. – 400 с.

Дополнительная литература:

- **Босс В.** Лекции по математике. Т. 6: Алгоритмы, логика, вычислимость. От Диофанта до Тьюринга и Геделя. Либроком, УРСС, 2012. – 2008 с.
- **Верещагин Н.К., Шень А.** Вычислимые функции. МЦНМО, 2012. – 160 с.
- **Гринченков Д.В., Потоцкий С.И.** Математическая логика и теория алгоритмов для программистов. М.: КноРус, 2012. – 206 с.
- **Мальцев А.И.** Алгоритмы и рекурсивные функции. М.: Наука, Физматлит, 1986. – 392 с.
- **Черч А.** Введение в математическую логику. Том 1. Либроком, 2009. – 482 с.
- **Хаггарти Р., Шлипф Дж., Уайтрайдс С.** Дискретная математика для программистов. Бином, Лаборатория знаний, 2010. – 632 с.

◆ Тема 12. Меры сложности алгоритмов.

Содержание лекционных занятий.

Понятие сложности алгоритмов и вычислений, эффективные алгоритмы. Легко и трудно разрешимые задачи. Полиномиальная эквивалентность. Недетерминированные алгоритмы. Недетерминированная машина Тьюринга. Классы задач P и NP. NP – полные и NP – трудные задачи. Квантовый компьютер и квантовые вычисления.

Содержание практических занятий.

Решение задач на доказательство полиномиальной эквивалентности алгоритмов.

Основная литература:

- **Андерсон Дж.** Дискретная математика и комбинаторика. М.: Вильямс, 2004. – 960 с.
- **Новиков Ф.А.** Дискретная математика для программистов. СПб.: Питер, 2008. – 384 с.
- **Хаггарти Р.** Дискретная математика для программистов. Техносфера, 2012. – 400 с.

Дополнительная литература:

- **Абрамов С.А.** Лекции о сложности алгоритмов. МЦНМО, 2012. – 248 с.
- **Босс В.** Лекции по математике. Т. 6: Алгоритмы, логика, вычислимость. От Диофанта до Тьюринга и Геделя. Либроком, УРСС, 2012. – 2008 с.
- **Верещагин Н.К., Шень А.** Вычислимые функции. МЦНМО, 2012. – 160 с.
- **Гринченков Д.В., Потоцкий С.И.** Математическая логика и теория алгоритмов для программистов. М.: КноРус, 2012. – 206 с.
- **Гуц А.К.** Математическая логика и теория алгоритмов. Либерком, 2009. – 120 с.
- **Набебин А.А., Кораблин Ю.П.** Математическая логика и теория алгоритмов. Научный мир, 2008. – 344 с.
- **Непейвода Н.Н.** Прикладная логика. – Новосибирск, НГУ, 2000. - 494 с.

- Новиков Ф.А. Дискретная математика. Питер, 2012. – 400 с.

◆ Тема 13. Основы теории информации.

Содержание лекционных занятий.

Кодирование информации. Блоковые коды. Префиксные коды. Кома-код. Код Грэя. Расстояние Хемминга. Коды, обнаруживающие ошибки. Коды, исправляющие ошибки. Код Хаффмана. Информационный объем сообщения. Формула Хартли. Информация, вероятность, энтропия. Формула Шеннона.

Содержание практических занятий.

Решение задач на определение информационного объема сообщения. Решение задач на оптимальное кодирование информации.

Основная литература:

- Авдошин С.М., Набебин А.А. Дискретная математика. Модулярная алгебра, криптография, кодирование. – М.: ДМК Пресс, 2017. – 352 с.
- Андерсон Дж. Дискретная математика и комбинаторика. М.: Вильямс, 2004. – 960 с.
- Андреева Е.В., Босова Л.Л., Фалина И.Н. Математические основы информатики. М.: Бином, 2007. – 328 с.
- Новиков Ф.А. Дискретная математика для программистов. СПб.: Питер, 2008. – 384 с.
- Хаггарти Р. Дискретная математика для программистов. Техносфера, 2012. – 400 с.

Дополнительная литература:

- Романовский И.В. Дискретный анализ. БХВ-Петербург, 2008. – 336 с.
- Смолин Ю.Н. Числовые системы. Флинта, Наука. -2009. – 112 с.
- Хаггарти Р., Шлипф Дж., Уайтсайд С. Дискретная математика для программистов. Бином, Лаборатория знаний, 2010. – 632 с.

◆ Тема 14. Системы счисления.

Содержание лекционных занятий.

Позиционные системы с натуральным основанием. Представление. Арифметические операции. Алгоритмы перевода чисел из одной системы счисления в другую. Смешанные системы счисления. Нетрадиционные системы счисления: симметричные и ассиметричные, уравновешенная троичная, с отрицательным основанием, негодвоичная, фибоначчиевая, факториальная, остаточных классов.

Содержание практических занятий.

Решение задач на применение различных алгоритмов для перевода из одной системы счисления в другую. Выполнение арифметических операций в различных системах счисления.

Основная литература:

- Андерсон Дж. Дискретная математика и комбинаторика. М.: Вильямс, 2004. – 960 с.
- Андреева Е.В., Босова Л.Л., Фалина И.Н. Математические основы информатики. М.: Бином, 2007. – 328 с.
- Новиков Ф.А. Дискретная математика для программистов. СПб.: Питер, 2008. – 384 с.
- Хаггарти Р. Дискретная математика для программистов. Техносфера, 2012. – 400 с.

Дополнительная литература:

- Гринченков Д.В., Потоцкий С.И. Математическая логика и теория алгоритмов для программистов. М.: КноРус, 2012. – 206 с.
- Новиков Ф.А. Дискретная математика. Питер, 2012. – 400 с.
- Романовский И.В. Дискретный анализ. БХВ-Петербург, 2008. – 336 с.
- Смолин Ю.Н. Числовые системы. Флинта, Наука. -2009. – 112 с.

- **Хаггарти Р., Шлипф Дж., Уайтсайдс С.** Дискретная математика для программистов. Бином, Лаборатория знаний, 2010. – 632 с.

◆ **Тема 15. Форматы представления информации в компьютере.**

Содержание лекционных занятий.

Стандарт IEEE 754-2008. Представление целых положительных, отрицательных и беззнаковых чисел. Прямой и дополнительный код. Представление вещественных чисел. Форматы для представления вещественных чисел со скрытой единицей. Представление текстовой информации. Представление графической информации. Представление звуковой информации. Методы сжатия информации.

Содержание практических занятий.

Решение задач на представление чисел в компьютере и выполнение операций в дополнительном коде. Перевод вещественных чисел в компьютерное представление и обратно. Нормализованное, ненормализованное и денормализованное представление вещественных чисел. Переопределение и исчезновение порядка. Специальные коды INF и NAN.

Основная литература:

- **Андерсон Дж.** Дискретная математика и комбинаторика. М.: Вильямс, 2004. – 960 с.
- **Андреева Е.В., Босова Л.Л., Фалина И.Н.** Математические основы информатики. М.: Бином, 2007. – 328 с.
- **Новиков Ф.А.** Дискретная математика для программистов. СПб.: Питер, 2008. – 384 с.
- **Хаггарти Р.** Дискретная математика для программистов. Техносфера, 2012. – 400 с.

Дополнительная литература:

- **Романовский И.В.** Дискретный анализ. БХВ-Петербург, 2008. – 336 с.
- **Хаггарти Р., Шлипф Дж., Уайтсайдс С.** Дискретная математика для программистов. Бином, Лаборатория знаний, 2010. – 632 с.
- **IEEE Std. 754-2008.** Standard for Floating-Point Arithmetic. – 58 р.

◆ **Тема 16. Вычислительная погрешность.**

Содержание лекционных занятий.

Приближенное представление вещественных чисел. Абсолютная и относительная погрешность. Погрешность выполнения арифметических операций. Аксиоматическое построение множества действительных чисел. Ошибки перевода вещественных чисел из десятичной системы в двоичную систему счисления. Ошибки представления. Ошибки округления. Ошибки сдвига и компенсации при выполнении арифметических операций.

Содержание практических занятий.

Решение задач на определение вычислительной погрешности. Вычислительная устойчивость численных алгоритмов.

Основная литература:

- **Андерсон Дж.** Дискретная математика и комбинаторика. М.: Вильямс, 2004. – 960 с.
- **Андреева Е.В., Босова Л.Л., Фалина И.Н.** Математические основы информатики. М.: Бином, 2007. – 328 с.
- **Новиков Ф.А.** Дискретная математика для программистов. СПб.: Питер, 2008. – 384 с.
- **Хаггарти Р.** Дискретная математика для программистов. Техносфера, 2012. – 400 с.

Дополнительная литература:

- **Романовский И.В.** Дискретный анализ. БХВ-Петербург, 2008. – 336 с.
- **Хаггарти Р., Шлипф Дж., Уайтсайдс С.** Дискретная математика для программистов. Бином, Лаборатория знаний, 2010. – 632 с.
- **IEEE Std. 754-2008.** Standard for Floating-Point Arithmetic. – 58 р.

◆ Тема 17. Функции и отношения.

Содержание лекционных занятий.

Бинарные отношения и их свойства. Соответствия и функции. Изоморфизм и гомоморфизм отношений. Композиция отношений. Степень отношения. Ядро отношения. Отношение эквивалентности. Классы эквивалентности. Фактор множества. Отношения порядка. Замыкание отношений.

Содержание практических занятий.

Операции над отношениями. Примеры отношений. Граф бинарного отношения. Степени вершин графа. Матрица смежностей (соседства вершин) и матрица инциденций (принадлежности вершин ребрам и ребер вершинам). Алгоритм поиска кратчайшего пути между вершинами в нагруженном связном ориентированном графе.

Основная литература:

- **Гаврилов Г.П., Сапоженко А.А.** Сборник задач по дискретной математике. М.: Наука, 1977. - 368с.
- **Кузнецов О.П., Адельсон-Вельский Г.М.** Дискретная математика для инженера. М.: Энергоатомиздат, 1988. - 480с.
- **Набебин А.А.** Дискретная математика. М.: Научный мир, 2010. 512с.
- **Набебин А.А.** Сборник заданий по дискретной математике. М.: Научный мир, 2009. 280с.
- **Новиков Ф.А.** Дискретная математика для программистов. СПб.: Питер, 2001.
- **Харари Ф.** Теория графов. М.: Мир, 1873. 300 с.
- **Яблонский С.В.** Введение в дискретную математику. М.: Наука, 1986. 384с.

Дополнительная литература:

- **Алексеев В.Б.** Лекции по дискретной математике. М.: Изд. отд. Фак. ВМиК МГУ им. М.В.Ломоносова, 2004. 74 с.
- **Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В.** Основы криптографии: Учебное пособие, 2-е изд., испр. и доп. М.: "Гелиос АРВ", 2002. 480с
- **Ахо А., Ульман Дж.** Теория синтаксического анализа, перевода и компиляции. Том 1, М.: Мир, 1978. 613с. Том 2, М.: Мир, 1978. 488с.
- **Биркгоф Г., Барти Т.** Современная прикладная алгебра. М.: Мир, 1976. 400 с.
- **Биркгоф Г.** Теория решеток. М.: Наука, 1984. 568 с.
- **Зыков А.А.** Основы теории графов. М.: Наука, 1987. 384 с.
- **Калужнин Л.А., Сущанский В.И.** Преобразования и перестановки. М.: Наука, 1985. 160 с.
- **Кон П.** Универсальная алгебра. М.: Мир, 1968. 352 с.
- **Кофман А.** Введение в прикладную комбинаторику. М.: Наука, 1975. 480 с.
- **Лидл Р., Нидеррайтер Г.** Конечные поля. М.: Мир, 1988. 820 с.
- **Питерсон У.** Коды, исправляющие ошибки. М.: Мир, 1964. 339с.
- **Риордан Дж.** Введение в комбинаторный анализ. М.: ИЛ, 1963. 288 с.
- **Рыбников К.А.** Введение в комбинаторный анализ. М.: Изд-во Моск. ун-та. 1985. 308 с.
- **Уилсон Р.** Введение в теорию графов. М.: Мир, 1977. 208 с.
- **Хантор Р.** Проектирование и конструирование компиляторов. М.: Финансы и статистика. 1984. 232с.

◆ Тема 18. Основы теории графов.

Содержание лекционных занятий.

Графы, мультиграфы, псевдографы, орграфы. Изоморфизм графов. Способы задания графов. Операции над графиками. Маршруты, цепи, циклы. Ациклический граф. Топологическая сортировка. Расстояния между вершинами. Диаметр, радиус, центр графа.

Содержание практических занятий.

Алгоритм топологической сортировки. Алгоритм вычисления расстояния между всеми парами вершин. Нахождение диаметра, радиуса и центров графа.

Основная литература:

- **Гаврилов Г.П., Сапоженко А.А.** Сборник задач по дискретной математике. М.: Наука, 1977. 368с.
- **Горбатов В.В.** Фундаментальные основы дискретной математики. М.: Наука, Физматлит, 1999.
- **Набебин А.А.** Дискретная математика. М.: Научный мир, 2010. 512с.
- **Набебин А.А.** Сборник заданий по дискретной математике. М.: Научный мир, 2009. 280с.
- **Харари Ф.** Теория графов. М.: Мир, 1873. 300 с.

Дополнительная литература:

- **Алексеев В.Б.** Лекции по дискретной математике. М.: Изд. отд. Фак. ВМиК МГУ им. М.В.Ломоносова, 2004. 74 с.
- **Биркгоф Г., Барти Т.** Современная прикладная алгебра. М.: Мир, 1976. 400 с.
- **Биркгоф Г.** Теория решеток. М.: Наука, 1984. 568 с.
- **Зыков А.А.** Основы теории графов. М.: Наука, 1987. 384 с.
- **Калужнин Л.А., Сущанский В.И.** Преобразования и перестановки. М.: Наука, 1985. 160 с.
- **Кофман А.** Введение в прикладную комбинаторику. М.: Наука, 1975. 480 с.
- **Лидл Р., Нидеррайтер Г.** Конечные поля. М.: Мир, 1988. 820 с.
- **Риордан Дж.** Введение в комбинаторный анализ. М.: ИЛ, 1963. 288 с.
- **Рыбников К.А.** Введение в комбинаторный анализ. М.: Изд-во Моск. ун-та. 1985. 308 с.
- **Уилсон Р.** Введение в теорию графов. М.: Мир, 1977. 208 с.
- **Яблонский С.В.** Введение в дискретную математику. М.: Наука, 1986. 384с.

◆ Тема 19. Сильная и слабая связность.

Содержание лекционных занятий.

Компоненты связности. Точки сочленения. Вершинная и реберная связность. Мосты и блоки. Меры связности. Обходы графов. Циклы Эйлера, де Брейна, Гамильтона. N-арные коды Грэя.

Содержание практических занятий.

Два алгоритма построения циклов Эйлера. Алгоритм построения цикла де Брюйна. Циклы Гамильтона и коды Грэя.

Основная литература:

- **Андерсон Дж.** Дискретная математика и комбинаторика. М.: Вильямс, 2003.
- **Набебин А.А.** Дискретная математика. М.: Научный мир, 2010. 512с.
- **Набебин А.А.** Сборник заданий по дискретной математике. М.: Научный мир, 2009. 280с.
- **Новиков Ф.А.** Дискретная математика для программистов. СПб.: Питер, 2001.
- **Харари Ф.** Теория графов. М.: Мир, 1873. 300 с.
- **Menezes A., van Oorshot P., Vanstone S.** Handbook of applied cryptography. CRC Press. 1996. 780 p. Internet address: www.cacr.math.uwaterloo.ca/ha

Дополнительная литература:

- **Алексеев В.Б.** Лекции по дискретной математике. М.: Изд. отд. Фак. ВМиК МГУ им. М.В.Ломоносова, 2004. 74 с.
- **Биркгоф Г., Барти Т.** Современная прикладная алгебра. М.: Мир, 1976. 400 с.
- **Биркгоф Г.** Теория решеток. М.: Наука, 1984. 568 с.
- **Зыков А.А.** Основы теории графов. М.: Наука, 1987. 384 с.
- **Калужнин Л.А., Сущанский В.И.** Преобразования и перестановки. М.: Наука, 1985. 160 с.
- **Кофман А.** Введение в прикладную комбинаторику. М.: Наука, 1975. 480 с.
- **Риордан Дж.** Введение в комбинаторный анализ. М.: ИЛ, 1963. 288 с.
- **Рыбников К.А.** Введение в комбинаторный анализ. М.: Изд-во Моск. ун-та. 1985. 308 с.
- **Уилсон Р.** Введение в теорию графов. М.: Мир, 1977. 208 с.

♦ Тема 20. Функциональные и контрфункциональные графы.

Содержание лекционных занятий.

Дерево и лес. Характеристические свойства деревьев. Каркасы (остовы) и хорды в связном графе. Ориентированные, упорядоченные, бинарные деревья. Алгоритмы обхода деревьев.

Содержание практических занятий.

Кодирование функциональных и контрфункциональных графов, ориентированных и неориентированных деревьев в компьютере. Представление произвольных ориентированных деревьев в виде бинарных. Алгоритмы обхода деревьев.

Основная литература:

- **Андерсон Дж.** Дискретная математика и комбинаторика. М.: Вильямс, 2003.
- **Гавrilov Г.П., Сапоженко А.А.** Сборник задач по дискретной математике. М.: Наука, 1977. 368с.
- **Набебин А.А.** Дискретная математика. М.: Научный мир, 2010. 512с.
- **Набебин А.А.** Сборник заданий по дискретной математике. М.: Научный мир, 2009. 280с.
- **Новиков Ф.А.** Дискретная математика для программистов. СПб.: Питер, 2001.
- **Харари Ф.** Теория графов. М.: Мир, 1873. 300 с.

Дополнительная литература:

- **Алексеев В.Б.** Лекции по дискретной математике. М.: Изд. отд. Фак. ВМиК МГУ им. М.В.Ломоносова, 2004. 74 с.
- **Биркгоф Г., Барти Т.** Современная прикладная алгебра. М.: Мир, 1976. 400 с.
- **Биркгоф Г.** Теория решеток. М.: Наука, 1984. 568 с.
- **Зыков А.А.** Основы теории графов. М.: Наука, 1987. 384 с.
- **Калужнин Л.А., Сущанский В.И.** Преобразования и перестановки. М.: Наука, 1985. 160 с.
- **Кофман А.** Введение в прикладную комбинаторику. М.: Наука, 1975. 480 с.
- **Риордан Дж.** Введение в комбинаторный анализ. М.: ИЛ, 1963. 288 с.
- **Рыбников К.А.** Введение в комбинаторный анализ. М.: Изд-во Моск. ун-та. 1985. 308 с.
- **Уилсон Р.** Введение в теорию графов. М.: Мир, 1977. 208 с.

♦ Тема 21. Фундаментальные системы циклов и коциклов.

Содержание лекционных занятий.

Циклы в графах. Линейное пространство бинарных наборов. Линейное пространство подграфов данного графа. Подпространство четных подграфов. Циклический и коциклический ранг графа (цикломатическое и коцикломатическое число). Матричная теорема Киркгофа о деревьях. Алгоритм построения фундаментальной системы циклов в графе.

Содержание практических занятий.

Построение фундаментальной системы циклов, соответствующее множество хорд, каркаса, всех фундаментальных разрезов с помощью алгоритма удаления циклических ребер в ненагруженном связном графе.

Основная литература:

- **Андерсон Дж.** Дискретная математика и комбинаторика. М.: Вильямс, 2003.
- **Гавrilov Г.П., Сапоженко А.А.** Сборник задач по дискретной математике. М.: Наука, 1977. 368с.
- **Горбатов В.В.** Фундаментальные основы дискретной математики. М.: Наука, Физматлит, 1999.
- **Набебин А.А.** Дискретная математика. М.: Научный мир, 2010. 512с.
- **Набебин А.А.** Сборник заданий по дискретной математике. М.: Научный мир, 2009. 280с.
- **Новиков Ф.А.** Дискретная математика для программистов. СПб.: Питер, 2001.
- **Харари Ф.** Теория графов. М.: Мир, 1873. 300 с.

Дополнительная литература:

- **Алексеев В.Б.** Лекции по дискретной математике. М.: Изд. отд. Фак. ВМиК МГУ им. М.В.Ломоносова, 2004. 74 с.

- **Зыков А.А.** Основы теории графов. М.: Наука, 1987. 384 с.
- **Калужнин Л.А., Сущанский В.И.** Преобразования и перестановки. М.: Наука, 1985. 160 с.
- **Кон П.** Универсальная алгебра. М.: Мир, 1968. 352 с.
- **Коффман А.** Введение в прикладную комбинаторику. М.: Наука, 1975. 480 с.
- **Уилсон Р.** Введение в теорию графов. М.: Мир, 1977. 208 с.

◆ **Тема 22. Алгоритмы на графах.**

Содержание лекционных занятий.

Алгоритмы поиска в глубину и ширину. Взвешенные графы. Алгоритмы Крускала и Прима построения минимального остовного дерева. Алгоритмические задачи траекторного типа во взвешенном графе. Обобщенный алгоритм Дейкстры. Обобщенное уравнение Беллмана-Маслова. Обобщенный алгоритм Флойда-Уоршала.

Содержание практических занятий.

Алгоритм построения компонент связности. Построение минимальных остовных деревьев в графе. Построение кратчайших, наиболее вероятных, минимаксных путей и путей с максимальной пропускной способностью.

Основная литература:

- **Горбатов В.В.** Фундаментальные основы дискретной математики. М.: Наука, Физматлит, 1999.
- **Кузнецов О.П., Адельсон-Вельский Г.М.** Дискретная математика для инженера. М.: Энергоатомиздат, 1988. 480с.
- **Набебин А.А.** Дискретная математика. М.: Научный мир, 2010. 512с.
- **Набебин А.А.** Сборник заданий по дискретной математике. М.: Научный мир, 2009. 280с.
- **Харари Ф.** Теория графов. М.: Мир, 1873. 300 с.

Дополнительная литература:

- **Алексеев В.Б.** Лекции по дискретной математике. М.: Изд. отд. Фак. ВМиК МГУ им. М.В.Ломоносова, 2004. 74 с.
- **Зыков А.А.** Основы теории графов. М.: Наука, 1987. 384 с.
- **Уилсон Р.** Введение в теорию графов. М.: Мир, 1977. 208 с.

◆ **Тема 23. Двудольные графы.**

Содержание лекционных занятий.

Паросочетания. Алгоритм построения совершенного паросочетания для двудольного графа. Системы различных представителей для конечного семейства конечных множеств (трансверсал). Теорема Холла о совершенных паросочетаниях.

Содержание практических занятий.

Построение совершенного паросочетания для двудольного графа. Вычисление системы различных представителей для конечного семейства конечных множеств.

Основная литература:

- **Горбатов В.В.** Фундаментальные основы дискретной математики. М.: Наука, Физматлит, 1999.
- **Кузнецов О.П.** Дискретная математика для инженеров. Книга по требованию, 2012. – 410 с.
- **Набебин А.А.** Дискретная математика. М.: Научный мир, 2010. 512с.
- **Набебин А.А.** Сборник заданий по дискретной математике. М.: Научный мир, 2009. 280с.
- **Новиков Ф.А.** Дискретная математика для программистов. СПб.: Питер, 2001.

Дополнительная литература:

- **Алексеев В.Б.** Лекции по дискретной математике. М.: Изд. отд. Фак. ВМиК МГУ им. М.В.Ломоносова, 2004. 74 с.
- **Зыков А.А.** Основы теории графов. М.: Наука, 1987. 384 с.
- **Уилсон Р.** Введение в теорию графов. М.: Мир, 1977. 208 с.

◆ Тема 24. Планарные графы.

Содержание лекционных занятий.

Укладка графа. Плоские графы. Эйлерова характеристика (формула Эйлера). Графы K_5 и $K_{3,3}$. Критерий планарности Понtryгина-Куратовского.

Содержание практических занятий.

Алгоритмы укладки графа на плоскость.

Основная литература:

- **Гаврилов Г.П., Сапоженко А.А.** Сборник задач по дискретной математике. М.: Наука, 1977. 368с.
 - **Липский В.** Комбинаторика для программистов. М.: Мир, 1988. 213 с.
 - **Набебин А.А.** Дискретная математика. М.: Научный мир, 2010. 512с.
 - **Набебин А.А.** Сборник заданий по дискретной математике. М.: Научный мир, 2009. 280с.
 - **Харари Ф.** Теория графов. М.: Мир, 1873. 300 с.
- Дополнительная литература:
- **Алексеев В.Б.** Лекции по дискретной математике. М.: Изд. отд. Фак. ВМиК МГУ им. М.В.Ломоносова, 2004. 74 с.
 - **Зыков А.А.** Основы теории графов. М.: Наука, 1987. 384 с.
 - **Уилсон Р.** Введение в теорию графов. М.: Мир, 1977. 208 с.

◆ Тема 25. Раскраска графов.

Содержание лекционных занятий.

Хроматическое число и хроматический класс. Верхняя и нижняя оценка хроматического числа. Внутренне и внешне устойчивые множества вершин графа. Оптимальная раскраска вершин графа. Раскрашивание планарных графов. Теоремы о пяти и о четырех красках.

Содержание практических занятий.

Алгоритмы вычисления в неориентированных и ориентированных графах *a)* все максимальные и наибольшие внутренне устойчивые (независимые) множества вершин; *b)* все минимальные и наименьшие внешне устойчивые (доминирующие) множества вершин. Оптимальная раскраска вершин графа.

Основная литература:

- **Гаврилов Г.П., Сапоженко А.А.** Сборник задач по дискретной математике. М.: Наука, 1977. 368с.
 - **Набебин А.А.** Сборник заданий по дискретной математике. М.: Научный мир, 2009. 280с.
 - **Новиков Ф.А.** Дискретная математика для программистов. СПб.: Питер, 2001.
 - **Харари Ф.** Теория графов. М.: Мир, 1873. 300 с.
 - **Яблонский С.В.** Введение в дискретную математику. М.: Наука, 1986. 384с.
- Дополнительная литература:
- **Зыков А.А.** Основы теории графов. М.: Наука, 1987. 384 с.
 - **Кристофидес Н.** Теория графов: алгоритмический подход. М.: МИР, 1978. 430с.
 - **Рыбников К.А.** Введение в комбинаторный анализ. М.: Изд-во Моск. ун-та. 1985. 308 с.
 - **Уилсон Р.** Введение в теорию графов. М.: Мир, 1977. 208 с.

◆ Тема 26. Потоки в сетях.

Содержание лекционных занятий.

Двухполюсные сети. Дивергенция. Разрезы (сечения). Величина потока и пропускная способность сети. Максимальный поток. Теорема Форда-Фалкерсона о максимальном потоке. Алгоритм построения максимального потока в сети. Многополюсная сеть. Обобщенная задача о назначениях и обобщенная транспортная задача. Алгоритмы решения обобщенной задачи о назначениях и обобщенной транспортной задачи.

Содержание практических занятий.

Алгоритмы построения максимального потока минимальной стоимости. Алгоритмы решения максиминной транспортной задачи. Алгоритмы решения задачи об оптимальном назначении.

Основная литература:

- Гаврилов Г.П., Сапоженко А.А. Сборник задач по дискретной математике. М.: Наука, 1977. 368с.
 - Набебин А.А. Дискретная математика. М.: Научный мир, 2010. 512с.
 - Набебин А.А. Сборник заданий по дискретной математике. М.: Научный мир, 2009. 280с.
 - Новиков Ф.А. Дискретная математика для программистов. СПб.: Питер, 2001.
 - Харари Ф. Теория графов. М.: Мир, 1873. 300 с.
- Дополнительная литература:
- Кофман А. Введение в прикладную комбинаторику. М.: Наука, 1975. 480 с.
 - Уилсон Р. Введение в теорию графов. М.: Мир, 1977. 208 с.
 - Харари Ф., Палмер Э. Перечисление графов. М.; МИР, 1977. - 324с.

◆ Тема 27. Универсальные алгебры.

Содержание лекционных занятий.

Операция суперпозиции. Замыкания и подалгебры. Система образующих. Морфизмы, гомоморфизм и изоморфизм алгебр. N-арные отношения. Конгруэнции и фактор-алгебры. Группы, кольца, области целостности и поля. Векторные пространства. Решетки. Конечные группы, кольца и поля.

Содержание практических занятий.

Решетки частично упорядоченных подмножеств. Цепи и антицепи. Алгоритм Евклида и расширенных алгоритм Евклида на числах и полиномах.

Основная литература:

- Авдошин С.М., Набебин А.А. Дискретная математика. Модулярная алгебра, криптография, кодирование. – М.: ДМК Пресс, 2017. – 352 с.
- Андерсон Дж. Дискретная математика и комбинаторика. М.: Вильямс, 2003.
- Гаврилов Г.П., Сапоженко А.А. Сборник задач по дискретной математике. М.: Наука, 1977. 368с.
- Липский В. Комбинаторика для программистов. М.: Мир, 1988. 213 с.
- Набебин А.А. Дискретная математика. М.: Научный мир, 2010. 512с.
- Набебин А.А. Сборник заданий по дискретной математике. М.: Научный мир, 2009. 280с.
- Новиков Ф.А. Дискретная математика для программистов. СПб.: Питер, 2001.
- Харари Ф. Теория графов. М.: Мир, 1873. 300 с.

Дополнительная литература:

- Калужнин Л.А., Сущанский В.И. Преобразования и перестановки. М.: Наука, 1985. 160 с.
- Риордан Дж. Введение в комбинаторный анализ. М.: ИЛ, 1963. 288 с.
- Рыбников К.А. Введение в комбинаторный анализ. М.: Изд-во Моск. ун-та. 1985. 308 с.

◆ Тема 28. Матроиды.

Содержание лекционных занятий.

Матроиды. Базы и ранг матроида. Аксиоматики матроидов. Теорема о базах. Графовый матроид. Матроид Фано. Матроид паросочетаний. Матричный матроид. Жадный алгоритм. Теорема Радо-Эдмондса.

Содержание практических занятий.

Применение жадных алгоритмов для решения графовых задач.

Основная литература:

- Авдошин С.М., Набебин А.А. Дискретная математика. Модулярная алгебра, криптография, кодирование. – М.: ДМК Пресс, 2017. – 352 с.
 - Липский В. Комбинаторика для программистов. М.: Мир, 1988. 213 с.
 - Новиков Ф.А. Дискретная математика. Питер, 2012. – 400 с.
- Дополнительная литература:
- Емеличев В.А., Мельников О.И., Сарванов В.И., Тышкевич Р.И. Лекции по теории графов. М.: Наука, 1990.

◆ Тема 29. Сети Петри.

Содержание лекционных занятий.

Сети Петри. Операционная семантика сетей Петри. Поведенческие свойства сетей Петри. Проблема достижимости и покрытие. Граф достижимости и деревья Карпа-Миллера. Живость и ограниченность. Инварианты позиций и переходов сетей Петри.

Содержание практических занятий.

Построение графов достижимости и покрытия. Поиск инвариантов сетей Петри.

Основная литература:

- **Андерсон Дж.** Дискретная математика и комбинаторика. М.: Вильямс, 2003.
 - **Касьянов В. Н., Евстигнеев В. А.**, Графы в программировании: обработка, визуализация и применение. Издательство: БХВ – Петербург, 2003, 1104 стр.
- Дополнительная литература:
- **Котов В. Е.** Сети Петри. М: Наука, 1984, 160 с.
 - **Питерсон Дж.** Теория сетей Петри и моделирование систем. М: Мир, 1984, 264 с.

◆ Тема 30. Модулярная арифметика.

Содержание лекционных занятий.

Делимость. Простые числа. Решето Эратосфена. Факторизация целых чисел. Метод выделения множителей Ферма. Наибольший общий делитель. Расширенный алгоритм Евклида. Наименьшее общее кратное. Функция Мебиуса и Эйлера. Теоремы Эйлера и Ферма.

Содержание практических занятий.

Алгоритмические задачи модулярной арифметики.

Основная литература:

- **Авдошин С.М., Набедин А.А.** Дискретная математика. Модулярная алгебра, криптография, кодирование. – М.: ДМК Пресс, 2017. – 352 с.
- **Андерсон Дж.** Дискретная математика и комбинаторика. М.: Вильямс, 2003.
- **Гаврилов Г.П., Сапоженко А.А.** Сборник задач по дискретной математике. М.: Наука, 1977. 368с.
- **Липский В.** Комбинаторика для программистов. М.: Мир, 1988. 213 с.
- **Набедин А.А.** Дискретная математика. М.: Научный мир, 2010. 512с.
- **Набедин А.А.** Сборник заданий по дискретной математике. М.: Научный мир, 2009. 280с.

Дополнительная литература:

- **Калужнин Л.А., Сущанский В.И.** Преобразования и перестановки. М.: Наука, 1985. 160 с.
- **Кон П.** Универсальная алгебра. М.: Мир, 1968. 352 с.
- **Кофман А.** Введение в прикладную комбинаторику. М.: Наука, 1975. 480 с.
- **Риордан Дж.** Введение в комбинаторный анализ. М.: ИЛ, 1963. 288 с.
- **Рыбников К.А.** Введение в комбинаторный анализ. М.: Изд-во Моск. ун-та. 1985. 308 с.
- **Харари Ф.** Теория графов. М.: Мир, 1873. 300 с.

◆ Тема 31. Модулярная арифметика.

Содержание лекционных занятий.

Цепные и подходящие дроби. Алгоритм вычисления подходящих дробей. Решение линейных диофантовых уравнений. Полная и приведенная система вычетов. Решение сравнений. Китайская теорема об остатках.

Содержание практических занятий.

Алгоритмические задачи модулярной арифметики.

Основная литература:

- **Авдошин С.М., Набедин А.А.** Дискретная математика. Модулярная алгебра, криптография, кодирование. – М.: ДМК Пресс, 2017. – 352 с.
- **Андерсон Дж.** Дискретная математика и комбинаторика. М.: Вильямс, 2003.
- **Гаврилов Г.П., Сапоженко А.А.** Сборник задач по дискретной математике. М.: Наука, 1977. 368с.

- Набебин А.А. Дискретная математика. М.: Научный мир, 2010. 512с.
Дополнительная литература:
- Набебин А.А. Сборник заданий по дискретной математике. М.: Научный мир, 2009. 280с.
- Гаврилов Г.П., Сапоженко А.А. Сборник задач по дискретной математике. М.: Наука, 1977. - 368с.

◆ Тема 32. Элементы теории кодирования.

Содержание лекционных занятий.

Алфавитное кодирование. Префиксный код. Кодирование с минимальной избыточностью. Алгоритмы Фано и Хаффмена. Блоковые и сверточные коды. Хеммингово расстояние, Хемминговы сферы и корректирующая способность. Коды, обнаруживающие и исправляющие ошибки. Линейные блоковые коды. Порождающая и проверочная матрицы. Кодирование и декодирование линейных блоковых кодов. Коды Хэмминга. Двоичные циклические коды. Порождающий и проверочный полиномы.

Содержание практических занятий.

Построение кодов с минимальной избыточностью. Построение кодов исправляющих ошибки.

Основная литература:

- Авдошин С.М., Набебин А.А. Дискретная математика. Модулярная алгебра, криптография, кодирование. – М.: ДМК Пресс, 2017. – 352 с.
- Андерсон Дж. Дискретная математика и комбинаторика. М.: Вильямс, 2004. – 960 с.
- Набебин А.А. Дискретная математика. М.: Научный мир, 2010. - 512с.
- Набебин А.А. Сборник заданий по дискретной математике. М.: Научный мир, 2009. 280с.

Дополнительная литература:

- Биркгоф Г. Теория решеток. М.: Наука, 1984. - 568 с.
- Биркгоф Г., Барти Т. Современная прикладная алгебра. М.: Мир, 1976. - 400 с.
- Гаврилов Г.П., Сапоженко А.А. Сборник задач по дискретной математике. М.: Наука, 1977. - 368с.
- Горбатов В.В. Фундаментальные основы дискретной математики. М.: Наука, Физматлит, 1999.
- Калужнин Л.А., Сущанский В.И. Преобразования и перестановки. М.: Наука, 1985. - 160 с.
- Кон П. Универсальная алгебра. М.: Мир, 1968. 352 с.
- Лидл Р., Нидеррайтер Г. Конечные поля. М.: Мир, 1988. - 820 с.
- Липский В. Комбинаторика для программистов. М.: Мир, 1988. 213 с.

◆ Тема 33. Применение модулярной арифметики в криптографии.

Содержание лекционных занятий.

Симметричные и несимметричные крипtosистемы. Криптографические протоколы. Криптография с открытым ключом. Шифросистемы и электронная цифровая подпись. Хэш-функция. Проблема квадратичного вычета. Проблема дискретного логарифма. Проблема подмножества суммы.

Содержание практических занятий.

Построение крипtosистем с открытым ключом. Алгоритмы модулярной арифметики.

Основная литература:

- Авдошин С.М., Набебин А.А. Дискретная математика. Модулярная алгебра, криптография, кодирование. – М.: ДМК Пресс, 2017. – 352 с.
- Набебин А.А. Дискретная математика. М.: Научный мир, 2010. - 512с.
- Набебин А.А. Сборник заданий по дискретной математике. М.: Научный мир, 2009. - 280с.
- Новиков Ф.А. Дискретная математика. Питер, 2012. – 400 с.

Дополнительная литература:

- Гаврилов Г.П., Сапоженко А.А. Сборник задач по дискретной математике. М.: Наука, 1977. - 368с.
- Лидл Р., Нидеррайтер Г. Конечные поля. М.: Мир, 1988. - 820 с.
- Харари Ф. Теория графов. М.: Мир, 1873. - 300 с.

◆ Тема 33. Проблема RSA и применение эллиптических кривых в криптографии.

Содержание лекционных занятий.

Проблема факторизации целых чисел. Проблема RSA. Факторизация полиномов над конечным полем. Крипtosистема RSA. Крипtosистема ЭльГамаля. Обмен ключами по схеме Диффи-Хеллмана с использованием эллиптических кривых. Шифрование/дешифрование с использованием эллиптических кривых.

Содержание практических занятий.

Системы RSA, Эль-Гамаля, Диффи-Хеллмана.

Основная литература:

- Авдошин С.М., Набебин А.А. Дискретная математика. Модулярная алгебра, криптография, кодирование. – М.: ДМК Пресс, 2017. – 352 с.
- Набебин А.А. Дискретная математика. М.: Научный мир, 2010. - 512с.
- Набебин А.А. Сборник заданий по дискретной математике. М.: Научный мир, 2009. - 280с.
- Новиков Ф.А. Дискретная математика. Питер, 2012. – 400 с.

Дополнительная литература:

- Гаврилов Г.П., Сапоженко А.А. Сборник задач по дискретной математике. М.: Наука, 1977. - 368с.
- Лидл Р., Нидеррайтер Г. Конечные поля. М.: Мир, 1988. - 820 с.
- Харари Ф. Теория графов. М.: Мир, 1873. - 300 с.
-

◆ Тема 35. Элементы комбинаторики.

Содержание лекционных занятий.

Порождение комбинаторных конфигураций и их пересчет. Размещения, перестановки, сочетания без повторений и с повторениями. Подстановки, группа подстановок. Генерация перестановок. Биномиальные коэффициенты, треугольник Паскаля, генерация подмножеств. Разбиения. Числа Стирлинга первого и второго рода, число Белла. Принцип включения и исключения. Производящие функции для комбинаторных конфигураций и их чисел. Аппарат формальных степенных рядов.

Содержание практических занятий.

Генерация и подсчет комбинаторных объектов.

Основная литература:

- Набебин А.А. Дискретная математика. М.: Научный мир, 2010. - 512 с.
 - Набебин А.А. Сборник заданий по дискретной математике. М.: Научный мир, 2009. – 280 с.
 - Новиков Ф.А. Дискретная математика для программистов. СПб.: Питер, 2012. – 400 с.
- Дополнительная литература:
- Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии: Учебное пособие, 2-е изд., испр. и доп. М.: "Гелиос АРВ", 2002. 480 с.
 - Menezes A., van Oorshot P., Vanstone S. Handbook of applied cryptography. CRC Press. 1996. 780 p. Internet address: www.cacr.math.uwaterloo.ca/ha

◆ Тема 36. Числовые рекуррентные уравнения.

Содержание лекционных занятий.

Рекуррентные уравнения. Линейные рекуррентные уравнения (ЛРУ). Фундаментальная система решений. Общее решение ЛРУ с помощью фундаментальной системы решений. Стационарные ЛРУ (СЛРУ). Характеристический полином и характеристическое уравнение. Общее решение однородного и неоднородного СЛРУ. Частное решение неоднородного СЛРУ с правой частью – квазиполиномом.

Содержание практических занятий.

Решение числовых рекуррентных уравнений.

Основная литература:

- **Новиков Ф.А.** Дискретная математика для программистов. СПб.: Питер, 2012. – 400 с.
Дополнительная литература:
- **Берлекэмп Э.** Алгебраическая теория кодирования. М.: МИР, 1971. 250с.
- **Питерсон У.** Коды, исправляющие ошибки. М.: Мир, 1964. 339с.
- **Лидл Р., Нидеррайтер Г.** Конечные поля. М.: Мир, 1988. 820 с.
- **Яблонский С.В.** Введение в дискретную математику. М.: Наука, 1986. 384с.

8 Образовательные технологии

Для выполнения самостоятельной работы заданий предусмотрены следующие открытые онлайн-курсы:

- массовый открытый онлайн-курс (Coursera) «Введение в логику» (Introduction to Logic).
Доступ к курсу можно получить по ссылке:
<https://www.coursera.org/learn/logic-introduction>
Курс размещен на платформе массовых открытых онлайн-курсов Coursera.
При прохождении по ссылке необходимо пройти бесплатную регистрацию на сайте Coursera. После чего, необходимо зарегистрироваться на курс с помощью студенческой почты (заканчивается на @edu.hse.ru).
Пройти регистрацию на курс необходимо в первом месяце учебного года (сентябрь).
- открытый курс (MIT OpenCourseware) «Математика для компьютерных наук» (Mathematics for Computer Science, 6.042J / 18.062J)
Доступ к материалам курса можно получить по ссылке:
<http://ocw.mit.edu/courses/electrical-engineering-and-computer-science/6-042j-mathematics-for-computer-science-fall-2010/>
Курс размещен на открытой платформе MIT OpenCourseware.

9 Оценочные средства для текущего контроля и аттестации студента

9.1 Тематика заданий текущего контроля

Тематика первого домашнего задания, предлагаемого в первом модуле, - исследование комбинационных схем. В процессе выполнения первого домашнего задания студент должен продемонстрировать владение культурой мышления, способность к обобщению, анализу, восприятию информации, постановке цели и выбору путей её достижения, навыки работы с инструментальными средствами при выполнении домашнего задания, умение оформлять отчет по результатам выполнения домашнего задания.

Домашнее задание 1. "Исследование комбинационных схем".

Файлы, содержащие исходные данные для выполнения домашнего задания 1 по дисциплине «Дискретная математика», содержатся в системе LMS.

Доступ к системе осуществляется по ссылке <http://lms.hse.ru/>

Подраздел «Домашнее задание 1» раздела «Материал» содержит следующие файлы:

[HW1.pdf](#) - инструкции по выполнению домашнего задания (данный файл);

[list.pdf](#) - список студентов с номерами вариантов домашних заданий;

[data.pdf](#) – варианты исходных данных для выполнения домашнего задания;

[WinLogica.rar](#) – архив, содержащий программу WinLogica для построения и анализа комбинационных схем.

Порядок выполнения домашнего задания 1.

- Постройте таблицу истинности логической функции F

A	0	0	0	0	1	1	1	1
B	0	0	1	1	0	0	1	1
C	0	1	0	1	0	1	0	1
F	X_7	X_6	X_5	X_4	X_3	X_2	X_1	X_0

Вычислите десятичный номер функции по формуле
 $2^7X_7+2^6X_6+2^5X_5+2^4X_4+2^3X_3+2^2X_2+2^1X_1+2^0X_0$.

Значения функции $X_7, X_6, X_5, X_4, X_3, X_2, X_1, X_0$ удовлетворяют системе линейных уравнений в поле $GF(2)$, эквивалентной уравнению с десятичными коэффициентами и побитовой операцией сложения по модулю 2, обозначенной знаком \oplus . Уравнение выбирается из файла data.pdf по номеру варианта.

- Представьте таблицу истинности логической функции F в виде карты Карно

F	0	0	1	1	A
	0	1	1	0	B
0	X_7	X_5	X_1	X_3	
1	X_6	X_4	X_0	X_2	
	C				

- Выполните дизъюнктивные разложения Шеннона логической функции F , представленной таблицей истинности, по каждой из переменных А, В и С. Запишите соответствующие разложению аналитические представления логической функции F , обозначая каждую из функций двух переменных одной операцией.
- Запишите предельное дизъюнктивное разложение Шеннона логической функции F в виде СДНФ (совершенной дизъюнктивной нормальной формы).
- Используя представление логической функции F в виде карты Карно, найдите все минимальные ДНФ (дизъюнктивные нормальные формы).
- Используя ортогональность функций в дизъюнктивных разложениях Шеннона, получите из аналитических представлений, полученных в пп. 3-5, новые аналитические представления логической функции F .
- Выполните конъюнктивные разложения Шеннона логической функции F , представленной таблицей истинности, по каждой из переменных А, В и С. Запишите соответствующие разложению аналитические представления логической функции F , обозначая каждую из функций двух переменных одной операцией.
- Запишите предельное конъюнктивное разложение Шеннона логической функции F в виде СКНФ (совершенной конъюнктивной нормальной формы).
- Используя представление логической функции F в виде карты Карно, найдите все минимальные КНФ (конъюнктивные нормальные формы).
- Используя ортогональность функций в конъюнктивных разложениях Шеннона, получите из аналитических представлений, полученных в пп. 7-9, новые аналитические представления логической функции F .
- Вычислите производные логической функции F , представленной таблицей истинности, по каждой из переменных А, В и С. Запишите соответствующие производные аналитические представления, обозначая каждую из функций двух переменных одной операцией.
- Выполните разложения Рида логической функции F по каждой из переменных А, В и С в точках 0 и 1.

13. Выполните двойственные разложения Рида логической функции F по каждой из переменных А, В и С в точках 0 и 1.
14. Вычислите все смешанные производные функции F с помощью таблиц истинности.
15. Получите аналитические выражения для всех смешанных производных функции F в аналитическом виде, исходя из определения производной или пользуясь таблицей производных. Выражения должны содержать минимально возможное количество операций.
16. Разложите функцию F в ряд Маклорена в базисе {1, XOR, AND}.
17. Разложите функцию F в ряд Тейлора в каждой точке пространства в базисе {1, XOR, AND}.
18. Разложите функцию F в ряд Маклорена в базисе {0, EQV, OR}.
19. Разложите функцию F в ряд Тейлора в каждой точке пространства в базисе {0, EQV, OR}.

Пункты 20 и 21 домашнего задания выполняются с использованием программы WinLogica. Результаты работы программы сохраняются в файлах с расширениями *.wlgc. Файлы *.wlgc записываются в директорию с именем \odot , где \odot - трехзначный номер варианта. Сдаваемая директория является первой частью отчета по домашнему заданию и должна содержать 18 файлов с именами $\odot \bullet .wlgc$. Здесь \odot - трехзначный номер варианта, а \bullet - двузначный номер базиса. Для пункта 20 в качестве \bullet указывается 00. Для пункта 21 номера базисов определяются следующей таблицей

\bullet	Базис	Подпункты меню Контроль
00		00 – ОБЩИЙ
01	{ F_{08} }	01 – NOR
02	{ F_{14} }	02 – NAND
03	{ F_{02}, F_{09} }	03 – 0, IMP
04	{ F_{00}, F_{13} }	04 – 1, COIMP
05	{ F_{02}, F_{13} }	05 – IMP, COIMP
06	{ F_{06}, F_{13} }	06 – XOR, IMP
07	{ F_{02}, F_{12} }	07 – EQV, COIMPL
08	{ F_{12}, F_{13} }	08 – NOT, IMP
09	{ F_{01}, F_{12} }	09 – NOT, COIMP
10	{ F_{07}, F_{12} }	10 – NOT, OR
11	{ F_{02}, F_{15} }	11 – NOT, AND
12	{ F_{00}, F_{01}, F_{09} }	12 – 0, EQV, AND
13	{ F_{00}, F_{07}, F_{09} }	13 – 1, XOR, OR
14	{ F_{01}, F_{06}, F_{09} }	14 – 0, EQV, OR
15	{ F_{06}, F_{07}, F_{09} }	15 – 1, XOR, AND
16	{ F_{01}, F_{06}, F_{15} }	16 – XOR, EQV, OR
17	{ F_{06}, F_{07}, F_{15} }	17 – EQV, XOR, AND

Перед размещением архива в LMS обязательно проверьте корректность созданных Вами схем с помощью программы WinLogica, поочередно загружая файлы $\odot \bullet .wlgc$ и выбирая подпункты меню «Валидация» -> «Проверка соответствие базиса», соответствующие номеру базиса \bullet .

20. Использую в качестве начального представления аналитические представления функции F , полученные в пп. 3-19, выразите функцию F с помощью минимального количества операций. Используя законы двойного отрицания и де Моргана, получите другие аналитические представления функции F с таким же количеством операций. Создайте в программе WinLogica схему, реализующую функцию F . Схема должна содержать минимально возможное количество блоков. Сохраните результат в файле $\odot 00.wlgc$. Номер варианта \odot должен быть трехзначным. Загрузите файл $\odot 00.wlgc$. С помощью подпункта меню «Валидация» -> «Проверка соответствие базиса» -> «00 – ОБЩИЙ» проверьте правильность

созданной вами схемы. Используя пункт «Экспорт» меню «Файл» сохраните изображение схемы в виде файла одного из трех типов .png, .jpg или .bmp. Полученное изображение должно быть вставлено в пояснительную записку.

21. Использую в качестве начального представления аналитические представления функции F , полученные в п. 20, получите аналитические представления функции F в каждом из семнадцати базисов, таким образом, чтобы соответствующая схемная реализация содержала минимальное количество блоков. Создайте в программе WinLogica схемы, реализующие функцию F в каждом из семнадцати базисов. Схемы должны содержать минимально возможное количество блоков. Сохраните результаты в файлах $\textcircled{1}\textcircled{2}.\text{wlgc}$. Поочередно загружая файлы $\textcircled{1}\textcircled{2}.\text{wlgc}$, с помощью подпунктов меню «Валидация» -> «Проверка соответствие базиса», соответствующих символу $\textcircled{2}$, проверьте правильность созданных Вами схем. Используя пункт «Экспорт» меню «Файл» сохраните изображения схем в виде файлов одного из трех типов .png, .jpg или .bmp. Полученные изображения должны быть вставлены в пояснительную записку.
22. Вычислите условия переключения сигнала на выходе схемы, реализующей функцию F , при переключении сигналов на каждой паре её входов с помощью таблиц истинности.
23. Получите аналитические выражения условий переключения сигнала на выходе схемы, реализующей функцию F , при переключении сигналов на каждой паре её входов. Формулы должны содержать минимально возможное количество операций.
24. Вычислите условия переключения сигнала на выходе схемы, реализующей функцию F , при переключении сигналов на всех её входах с помощью таблиц истинности.
25. Получите аналитическое выражение условия переключения сигнала на выходе схемы, реализующей функцию F , при переключении сигналов на всех её входах. Формула должна содержать минимально возможное количество операций.
26. Определите принадлежность функции F к пяти замкнутым классам критерия Поста. Принадлежность функции к каждому замкнутому классу должна быть доказана.
27. Определите функции двух переменных, которые можно выразить через функцию F . Выразите через функцию F каждую функцию двух переменных или докажите невозможность такой записи.

Отчет по домашнему заданию состоит из двух частей, упакованных в один архив с именем $\textcircled{1}.\text{rar}$ или $\textcircled{1}.\text{zip}$, который выкладывается для проверки в подраздел «Домашнее задание № 1» раздела «Проекты». Здесь $\textcircled{1}$ – трехзначный номер варианта.

1. Первая часть содержит 18 файлов с именами $\textcircled{1}\textcircled{2}.\text{wlgc}$. Здесь $\textcircled{1}$ – трехзначный номер варианта, а $\textcircled{2}$ – двузначный номер базиса. Файлы с изображениями схем вкладывать в архив не нужно.
2. Вторая часть - пояснительная записка с именем $\textcircled{1}.\text{doc}$ или $\textcircled{1}.\text{docx}$, содержит описание выполненных пунктов домашнего задания. Она должна быть вложена в сдаваемый архив с именем $\textcircled{1}.\text{rar}$ или $\textcircled{1}.\text{zip}$. Обратите внимание, что пункты 20 и 21 пояснительной записи должны содержать графическое изображение схем. Кроме того пояснительная записка в распечатанном виде в обязательном порядке сдается преподавателю. Файл Образец оформления ДЗ.pdf, находящийся в подраздел «Домашнее задание 1» раздела «Материал», содержит образец оформления пояснительной записки.

Тематика второго домашнего задания, предлагаемого во втором модуле, - исследование моделей вычислений. В процессе выполнения второго домашнего задания студент должен продемонстрировать владение культурой мышления, способность к обобщению, анализу, восприятию информации, постановке цели и выбору путей её достижения, навыки работы с инструментальными средствами при выполнении домашнего задания, умение оформлять отчет по результатам выполнения домашнего задания.

Домашнее задание 2. "Исследование моделей вычислений".

Файлы, содержащие исходные данные для выполнения домашнего задания 2 по дисциплине «Дискретная математика», содержатся в системе LMS.

Доступ к системе осуществляется по ссылке <http://lms.hse.ru/>

Подраздел «Домашнее задание 2» раздела «Материал» содержит следующие файлы:

[HW2.pdf](#) - инструкции по выполнению домашнего задания (данный файл);

[list.pdf](#) - список студентов с номерами вариантов домашних заданий;

[data.pdf](#) – варианты исходных данных для выполнения домашнего задания;

[emt_setup.rar](#) – установочный файл Эмулятора Машины Тьюринга;

[post_setup.rar](#) – установочный файл Эмулятора Машины Поста;

[markov_setup.rar](#) – установочный файл Эмулятора алгоритмов Маркова;

[rf_seup.rar](#) – установочный файл Эмулятора рекурсивных функций.

Порядок выполнения домашнего задания 2.

1. Запишите алгоритм вычисления логической функции $F(A,B,C)$, найденной в домашнем задании 1, в форме программы для машины Тьюринга. Алгоритм должен вычислять логическую функцию F над битами целочисленных аргументов A , B и C , заданных в двоичной системе счисления. Один аргумент от другого должен отделяться символом $*$. Таким образом, входное слово для машины Тьюринга должно иметь вид $A*B*C$, где под слова A , B и C записываются в алфавите $\{0,1\}$. Коды чисел, соответствующие аргументам A , B и C в общем случае могут иметь различную длину. Результат побитового применения функции $F(A,B,C)$ должен формироваться на месте исходного слова и иметь длину, равную длине операнда, имеющего максимальное количество двоичных разрядов. Операнды меньшей длины считаются выровненными слева до длины аргумента, записанного максимальным количеством символов, символами 0. Выходное слово не должно содержать никаких других символов, кроме символов алфавита $\{0,1\}$ с помощью которых записан результат побитового применения функции $F(A,B,C)$. Алгоритм считается корректным, если в процессе его работы не образуется пустых символов внутри обрабатываемого слова. Внутри входного слова пустые символы также недопустимы. Если аргумент A , B или C отсутствует, он считается равным нулю. В начале работы алгоритма автомат должен находиться в состоянии, записанном в первой строке программы для машины Тьюринга, и видеть первый, самый левый, символ входного слова.
2. Запишите алгоритм вычисления логической функции $F(A,B,C)$, найденной в домашнем задании 1, в форме программы для машины Поста. Алгоритм должен вычислять логическую функцию F над битами целочисленных аргументов A , B и C , заданных в двоичной системе счисления. Один аргумент от другого должен отделяться символом $*$. Таким образом, входное слово для машины Поста должно иметь вид $A*B*C$, где под слова A , B и C записываются в алфавите $\{0,1\}$. Коды чисел, соответствующие аргументам A , B и C в общем случае могут иметь различную длину. Результат побитового применения функции $F(A,B,C)$ должен формироваться на месте исходного слова и иметь длину, равную длине операнда, имеющего максимальное количество двоичных разрядов. Операнды меньшей длины считаются выровненными слева до длины аргумента, записанного максимальным количеством символов, символами 0. Выходное слово не должно содержать никаких других символов, кроме символов алфавита $\{0,1\}$ с помощью которых записан результат побитового применения функции $F(A,B,C)$. Алгоритм считается корректным, если в процессе его работы не образуется пустых символов внутри обрабатываемого слова. Внутри входного слова пустые символы также недопустимы. Если аргумент A , B или C отсутствует, он считается равным нулю. В начале работы алгоритма автомат должен находиться в состоянии, записанном в первой строке программы для машины Поста, и видеть первый, самый левый, символ входного слова. Представление символов алфавита, обрабатываемого машиной Поста в виде последовательности помеченных и непомеченных ячеек ленты необходимо выбрать самостоятельно. Выбранная кодировка в обязательном порядке должна быть записана в

комментариях программы. Пустой символ при этом должен кодироваться последовательностью непомеченных ячеек ленты. В начальном состоянии автомата машины Поста должен видеть первую самую левую ячейку первого символа входного слова.

3. Запишите алгоритм вычисления логической функции $F(A,B,C)$, найденной в домашнем задании 1, в форме нормального алгоритма Маркова. Алгоритм должен вычислять логическую функцию F над битами целочисленных аргументов A , B и C , заданных в двоичной системе счисления. Один аргумент от другого должен отделяться символом $*$. Таким образом, входное слово для нормального алгоритма Маркова должно иметь вид $A*B*C$, где под слова A , B и C записываются в алфавите $\{0,1\}$. Коды чисел, соответствующие аргументам A , B и C в общем случае могут иметь различную длину. Результат побитового применения функции $F(A,B,C)$ должен формироваться на месте исходного слова и иметь длину, равную длине операнда, имеющего максимальное количество двоичных разрядов. Операнды меньшей длины считаются выровненными слева до длины аргумента, записанного максимальным количеством символов, символами 0. Выходное слово не должно содержать никаких других символов, кроме символов алфавита $\{0,1\}$ с помощью которых записан результат побитового применения функции $F(A,B,C)$. Если аргумент A , B или C отсутствует, он считается равным нулю.
4. Запишите алгоритм вычисления логической функции $F(A,B,C)$, найденной в домашнем задании 1, в форме частично-рекурсивной функции. Алгоритм должен вычислять логическую функцию F над битами целочисленных аргументов A , B и C , заданных в виде десятичных чисел без знака. Обращение к функции должно иметь вид $F_{\odot}(A,B,C)$, где \odot - номер варианта. Двоичные коды чисел, соответствующие аргументам A , B и C в общем случае могут иметь различную длину. Результат побитового применения функции $F(A,B,C)$ должен выводиться в виде десятичного числа без знака, и иметь длину в двоичной системе счисления, равную длине операнда, имеющего максимальное количество значащих двоичных разрядов. Операнды, имеющие меньшую длину в двоичной системе счисления, считаются выровненными слева до длины максимального аргумента, двоичными символами 0. Если аргумент равен нулю, то его длина в двоичной системе счисления считается равной единице.

Отчет по домашнему заданию состоит из пяти частей.

1. Файл с именем $\odot.alg$, представляющий собой описание алгоритма для эмулятора машины Тьюринга, выкладывается для проверки в системе LMS в подраздел «Домашнее задание № 2. Машина Тьюринга» раздела «Проекты». Здесь \odot – номер варианта.
2. Файл с именем $\odot.mpst$, представляющий собой описание алгоритма для эмулятора машины Поста, выкладывается для проверки в системе LMS в подраздел «Домашнее задание № 2. Машина Поста» раздела «Проекты». Здесь \odot – номер варианта.
3. Файл с именем $\odot.mrc$, представляющий собой описание алгоритма для эмулятора нормального алгоритма Маркова, выкладывается для проверки в системе LMS в подраздел «Домашнее задание № 2. Нормальный алгоритм Маркова» раздела «Проекты». Здесь \odot – номер варианта.
4. Файл с именем $\odot.rf$, представляющий собой описание алгоритма для эмулятора рекурсивных функций, выкладывается для проверки в системе LMS в подраздел «Домашнее задание № 2. Рекурсивные функции» раздела «Проекты». Здесь \odot – номер варианта.
5. Защита сделанных работ преподавателю в компьютерном классе.

Тематика третьего домашнего задания, предлагаемого в третьем модуле, - точные и приближенные алгоритмы решения NP-трудных задач оптимизации. В процессе выполнения третьего домашнего задания студент должен продемонстрировать владение культурой мышления, способность к обобщению, анализу, восприятию информации, постановке цели и выбору путей её достижения, навыки работы с инструментальными

средствами при выполнении домашнего задания, умение оформлять отчет по результатам выполнения домашнего задания.

Домашнее задание 3. "Исследование алгоритмов решения метрической задачи коммивояжера".

Файлы, содержащие исходные данные для выполнения домашнего задания 3 по дисциплине «Дискретная математика», содержатся в системе LMS.

Доступ к системе осуществляется по ссылке <http://lms.hse.ru/>

Подраздел «Домашнее задание 3» раздела «Материал» содержит следующие файлы:

HW3.pdf - инструкции по выполнению домашнего задания (данный файл);

list.pdf - список студентов с номерами вариантов домашних заданий;

data.pdf – варианты исходных данных для выполнения домашнего задания.

Порядок выполнения домашнего задания 3.

- На плоскости задано множество точек $V = \{1, 2, 3, 4, 5, 6\}$ своими координатами

$$(x_1, y_1) \quad (x_2, y_2) \quad (x_3, y_3) \quad (x_4, y_4) \quad (x_5, y_5) \quad (x_6, y_6)$$

Определите значения перечисленных переменных,
выбрав их из файла **data.pdf** по номеру своего варианта.

- Вычислите элементы d_{ij} весовой матрицы смежности графа $G = \langle V, V \times V \rangle$

$$D = \begin{pmatrix} d_{11} & d_{12} & d_{13} & d_{14} & d_{15} & d_{16} \\ d_{21} & d_{22} & d_{23} & d_{24} & d_{25} & d_{26} \\ d_{31} & d_{32} & d_{33} & d_{34} & d_{35} & d_{36} \\ d_{41} & d_{42} & d_{43} & d_{44} & d_{45} & d_{46} \\ d_{51} & d_{52} & d_{53} & d_{54} & d_{55} & d_{56} \\ d_{61} & d_{62} & d_{63} & d_{64} & d_{65} & d_{66} \end{pmatrix} \text{ по формуле } d_{ij} = |x_i - x_j| + |y_i - y_j|$$

- Обозначим через $S = \{p : V \rightarrow V \mid (p(1) = 1) \& (\forall i \in V)(\forall j \in V)((p(i) = p(j)) \Rightarrow (i = j))\}$ множество кодов всех гамильтоновых циклов $\nu = (p_1, p_2, p_3, p_4, p_5, p_6, p_1)$ графа G . Здесь p_i используется в качестве сокращенной записи для $p(i)$.

В этих обозначениях вес гамильтонова цикла $\nu \in S$ определяется его кодом $p_1 p_2 p_3 p_4 p_5 p_6$ по

$$\text{формуле } f(\nu) = \sum_{i=1}^5 d_{p_i p_{i+1}} + d_{p_6 p_1}.$$

Найдите, используя метод ветвей и границ, подмножество $S_o \subseteq S$ кодов $p_1 p_2 p_3 p_4 p_5 p_6$ всех гамильтоновых циклов $\nu \in S_o$, удовлетворяющих соотношению $(\exists f_o \in \mathbb{R}_+)(\forall \nu \in S_o)(f(\nu) = f_o) \& (\forall \nu \in S)(f(\nu) \geq f_o)$, т.е. кодов всех оптимальных гамильтоновых циклов являющихся решением задачи коммивояжера на графике G . Здесь f_o - вес оптимального гамильтонова цикла.

- Найдите приближенное решение задачи коммивояжера с помощью алгоритма Кристофида с временной сложностью $O(|V|^2)$. Постройте кратчайшее связывающее дерево $T = \langle V, E(T) \rangle$ графа G . Удвойте ребра дерева. В графике $\langle V, E(T) \parallel E(T) \rangle$ постройте Эйлеров цикл. Удалите повторения вершин Эйлерова цикла. Полученный гамильтонов цикл есть приближенное решение задачи коммивояжера. Оцените относительную точность полученного решения.
- Найдите приближенное решение задачи коммивояжера с помощью алгоритма Кристофида с временной сложностью $O(|V|^3)$. Постройте кратчайшее связывающее дерево

$T = \langle V, E(T) \rangle$ графа G . Постройте паросочетание $M = \langle V_H, E(M) \rangle$ минимального веса множества вершин $V_H \subseteq V$ нечетной степени дерева T . В графе $\langle V, E(T) \cup E(M) \rangle$ постройте Эйлеров цикл. Удалите повторения вершин Эйлерова цикла. Полученный гамильтонов цикл есть приближенное решение задачи коммивояжера. Оцените относительную точность полученного решения.

Отчет по домашнему заданию состоит из Пояснительной записи с именем $\textcircled{1}.doc$ (или $\textcircled{1}.pdf$), где $\textcircled{1}$ – трехзначный номер варианта, содержащей описание выполненных пунктов домашнего задания. Пояснительная записка выкладывается для проверки в подраздел «Домашнее задание № 3» раздела «Проекты» и в распечатанном виде сдается преподавателю. Файл Образец оформления ДЗ.pdf, находящийся в подраздел «Домашнее задание 3» раздела «Материал», содержит образец пояснительной записи.

Тематика четвертого домашнего задания, предлагаемого в четвертом модуле, - криптография и комбинаторика. В процессе выполнения четвертого домашнего задания студент должен продемонстрировать владение культурой мышления, способность к обобщению, анализу, восприятию информации, постановке цели и выбору путей её достижения, навыки работы с инструментальными средствами при выполнении домашнего задания, умение оформлять отчет по результатам выполнения домашнего задания.

Домашнее задание 4. "Криптография. Комбинаторика."

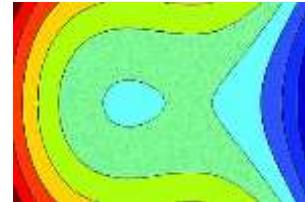
Исходные данные для выполнения домашнего задания 4 по дисциплине «Информатика, математическая логика и теория алгоритмов», состоят из

- [HW4.pdf](#) – инструкции по выполнению домашнего задания 4;
- [HW4_example_Part\[1-3\]](#) – шаблоны для оформления домашнего задания;
- Вариант задания.

Пример домашнего задания за 4 модуль прошлого года.

Часть 1. Эллиптическая криптография.

Криптографические методы основанные на арифметике эллиптических кривых над конечными полями получили большое распространение и признание в области компьютерной безопасности. Новые стандарты безопасности (Россия, США) переходят на использование криптографических алгоритмов, основанных на эллиптических кривых.



В варианте предоставлены параметры эллиптической кривой $y^2 = x^3 + ax + b$ над F_q :

- q — характеристика конечного числового поля;
- a, b — параметры эллиптической кривой;

и генератор эллиптической группы P .

Необходимо:

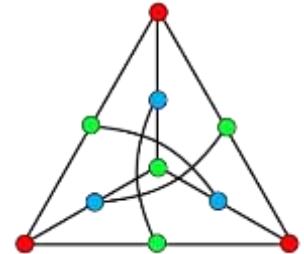
1. Нарисовать график кривой над вещественным полем вручную или используя любой инструмент (Wolfram Alpha, Sage, Maple, MathCAD, итп).
2. Проверить сингулярность кривой.
3. Выписать первые 10 точек, порождаемых генератором P ;
4. Вычислить порядок генератора P ;
5. Используя схему Эль-Гамала передать сообщение от Красной Шапочки к Бабушке. Параметры кривой и генератора использовать из предоставленного варианта.
 - a. Бабушка выбирает секретное число a и вычисляет точку $A = [a]P \in E(F_q)$;
 - b. Бабушка публикует точку A . Это ее открытый ключ. a — секретный ключ;

- c. Красная Шапочка представляет свое сообщение точкой $M \in E(F_q)$, выбирает произвольное число k , и вычисляет $B_1 = [k]P \in E(F_q)$ и $B_2 = M + [k]A \in E(F_q)$;
 - d. Красная Шапочка отправляет Бабушке шифр (B_1, B_2) через потенциально уязвимую линию;
 - e. Бабушка используя свой закрытый ключ a вычисляет $B_2 - [a]B_1 \in E(F_q)$. Предоставить объяснение почему Бабушка осуществляет $B_2 - [a]B_1$.
6. (*) Параметры кривой и генератора использовать из предоставленного варианта. Необходимо изучить следующую схему:
- a. Волк выбирает секретное число a и вычисляет точку $A = [a]P \in E(F_q)$;
 - b. Волк публикует точку A . Это его открытый ключ. a — секретный ключ;
 - c. Бармалей представляет свое сообщение точкой $(m_1, m_2) \in F_q^2$, выбирает произвольное число k , и вычисляет $B_1 = [k]P$ и $B_2 = [k]A$;
 - d. Бармалей представляет B_2 в виде $(x, y) \in E(F_q)$, вычисляет $c_1 = xm_1$ и $c_2 = ym_2$, и отправляет Волку шифр (B_1, c_1, c_2) ;
 - e. Предоставить объяснение как Волк, используя (B_1, c_1, c_2) и свой закрытый ключ, может расшифровать сообщение Бармалея (m_1, m_2) .

Во всех пунктах Вам необходимо предоставить все промежуточные шаги выполнения вычислений и давать необходимые комментарии по ходу вычислений. Промежуточные шаги выполнения вычислений и комментарии учитываются при оценивании и их отсутствие снижает результирующую оценку. В конце каждого пункта Вам необходимо отдельно выписать и явно указать, что является ответом. Если ответ для пункта не указан явно или не выписан отдельно, оценивание пункта не выполняется и пункт оценивается оценкой 0. Шаблон оформления работы представлен в файле HW4_example_Part1.pdf.

Часть 2. Комбинаторика.

Известно, что начальный толчок к развитию теория вероятности и комбинаторика получили при анализе головоломок и азартных игр. Начав с таких бытовых и развлекательных приложений, комбинаторика выросла в сложную и обширную область математики, а комбинаторные методы получили как практические применения — анализ и построение алгоритмов, генетика, статистика, так и теоретические — теория сложности, теория информации, математическая логика, теория вероятности.



В задании предоставлена конфигурация игры «Комбинаторный покер»:

- R — подмножество комбинаций, участвующих в игре (например, $R = \langle RF; SF; 3+2 \rangle$);
- X — карты, отсутствующие в колоде (например, $X = \langle C6; S7; D5; DK; S5 \rangle$);
- C — набор карт в руках (например, $C = \langle D6; D7; SJ \rangle$);
- A — искомая комбинация (например, $A=3+2$);
- S — колода карт, задана как полная колода D (52 карты) без карт из C и X (то есть $S = D - (C + X)$).

Существуют следующие комбинации:

- RF — Royal flush, 5 карт последовательных (T)-(A) рангов от 10 до туза одной масти;
- SF — Straight flush, 5 карт последовательных (n)-(n+4) рангов одной масти;
- 4K — Four of a kind, 4 карты одного (n) ранга;
- 3+2 — Full house, 3 карты (n) ранга и 2 карты (m) ранга, где $n \neq m$;
- FL — Flush, 5 карт одной масти;
- ST — Straight, 5 карт последовательных рангов (n)-(n+4), причем имеются разные масти;
- 3K — Three of a kind, 3 карты одного (n) ранга;

- 2+2 — Two pair, 2 карты (n) ранга и 2 карты (m) ранга, где $n \neq m$;
- 2K – Pair, 2 карты одного ранга.

При всех расчетах учитываются только комбинации из R . Остальные комбинации не учитываются.

Порядок на комбинациях: $RF > SF > 4K > 3 + 2 > FL > ST > 3K > 2 + 2 > 2K$.

Необходимо:

Рассчитать вероятность появления комбинации A (указана в варианте) в руках при извлечении дополнительных ($7 - |C|$) карт из колоды S.

Вам необходимо предоставить все промежуточные шаги выполнения вычислений и давать необходимые комментарии по ходу вычислений. Промежуточные шаги выполнения вычислений и комментарии учитываются при оценивании и их отсутствие снижает результирующую оценку. Для каждого промежуточного рассматриваемого множества комбинаций, Вам необходимо отдельно выписать и явно указать, что является числом возможных комбинаций данного типа. Если ответ не указан явно или не выписан отдельно, оценивание данного фрагмента работы не выполняется, и результирующая оценка снижается. Шаблон оформления работы представлен в файле HW4_example_Part2.pdf.

Часть 3. Обратный мультипликативный элемент.

Задан полином $P(x)$ из $Z_p[x]$.

В варианте предоставлены:

- p — характеристика числового поля коэффициентов;
- $P(x), F(x)$ — полиномы из $Z_p[x]$.

Необходимо найти мультипликативный обратный $Q(x)$ в $Z_p[x]/F(x)$ для полинома $P(x)$.



Отчет по домашнему заданию состоит из 4 частей.

1. Отчет по 1 части домашнего задания. Должен содержать:

- ФИО, № группы, № варианта;
- описание задания;
- параметры варианта;
- все промежуточные вычисления, указанные в части «Часть 1. Эллиптическая криптография».

Не забыть:

- комментарии как Вы находили точки представляющие сообщения;
- в задании (*) важно привести как шаги вычисления, так и те соображения, которые к ним привели. Без аргументации задание не засчитывается.

- код программы (скрипты Wolphram Alpha, C# код, итп) для промежуточных вычислений

Все артефакты (отчет, код программы) должны быть приложены к решению и их отсутствие приводит к снижению оценки.

2. Отчет по 2 части домашнего задания. Должен содержать:

- ФИО, № группы, № варианта;
- описание задания;
- параметры варианта;
- диаграмма Хассе (или диаграмма Эйлера — Венна) для комбинаций из R ;
- изображение колоды в виде таблицы (шаблон оформления в HW4_example_Part2);
- все промежуточные вычисления, указанные в части «Часть 2. Комбинаторика» и оформленные как в шаблоне HW4_example_Part2.

Не забыть:

- все промежуточные вычисления и промежуточные выводы;
- все применения формулы включения/исключения; исключения комбинаций из рассмотрения; распределение рангов или цветов должны быть обоснованы;
- код программы (скрипты Wolphram Alpha, C# код, итп) для промежуточных вычислений

Все артефакты (отчет, код программы) должны быть приложены к решению и их отсутствие приводит к снижению оценки.

3. Отчет по З части домашнего задания. Должен содержать:

- ФИО, № группы, № варианта;
- описание задания;
- параметры варианта;
- промежуточные вычисления и обязательно разложение;
- все промежуточные вычисления, указанные в части «Часть 3. Обратный мультипликативный элемент» и оформленные как в шаблоне HW4_example_Part2.

Не забыть:

- вычисление НОД;
- вычисление коэффициентов разложение;
- ответ и вывод должны быть обоснованным.

Все артефакты (отчет, код программы) должны быть приложены к решению и их отсутствие приводит к снижению оценки.

4. Защита решения частей преподавателю.

9.2 Вопросы для оценки качества освоения дисциплины

Примерный перечень вопросов к текущему и итоговому контролю для самопроверки студентов.

1. Сформулируйте законы Аристотеля.
2. Дайте определения равносильных формул, тавтологии, противоречия, выполнимости, опровергимой формулы.
3. Дайте определения предиката и квантора.
4. Сформулируйте законы де Моргана.
5. Приведите примеры изоморфных алгебр.
6. Сформулируйте классический принцип двойственности.
7. Опишите связь между булевой алгеброй и алгеброй Кантора.
8. Сформулируйте законы поглощения.
9. Сформулируйте законы Порецкого.
10. Сформулируйте законы склеивания.
11. Запишите формулы дизъюнктивного и конъюнктивного разложения Шеннона.
12. Запишите в общем виде совершенную дизъюнктивную нормальную форму и совершенную конъюнктивную нормальную форму логической функции трех переменных.
13. Сформулируйте прямое и двойственное определение ортогональности функций.
14. Запишите пары прямых и двойственных разложений Рида.
15. Запишите в общем виде полиномы Жегалкина для логической функции трех переменных.
16. Опишите возможные алгоритмы решения логических и теоретико-множественных уравнений.
17. Опишите возможные алгоритмы для решения систем линейных алгебраических уравнений в поле Галуа GF(2).

18. Дайте определение производной, производной по направлению и смешанной производной логической функции.
19. Запишите таблицу производных булевых функций.
20. Запишите в общем виде формулы для разложения булевой функции в ряд Тейлора и Макларена.
21. Приведите пример реализации триггера на логических элементах.
22. Дайте определения замкнутых классов логических функций. Приведите примеры.
23. Дайте определение полной системы булевых функций в сильном и слабом смысле. Приведите примеры.
24. Дайте определение базиса. Приведите примеры.
25. Сформулируйте теорему Поста.
26. Опишите алгоритм минимизация булевых функций в классе дизъюнктивных и конъюнктивных нормальных форм.
27. Опишите алгоритм минимизации частично-определенных функций с использованием карт Карно.
28. Опишите методы минимизаций булевых функций в заданных базисах.
29. Дайте определения автоматов Мили и Мура.
30. Напишите формулу для вычисления транзитивного и рефлексивного замыкания Клини.
31. Дайте определение и укажите способы описания регулярных выражений и регулярных языков.
32. Дайте определение префиксных, суффиксных и инфиксных кодов.
33. Укажите способы задания грамматик.
34. Опишите алгоритм минимизации автомата Мили.
35. Опишите алгоритм минимизации автомата Мура.
36. Приведите схему компьютера, как программно управляемого цифрового автомата.
37. Дайте определение аксиоматической системы.
38. Поясните полноту, непротиворечивость и разрешимость формализованного исчисления высказываний.
39. Приведите примеры независимой системы аксиом.
40. Опишите принцип дедукции.
41. Опишите метод резолюций.
42. Опишите метод Вонга.
43. Опишите натуральное исчисление.
44. Приведите примеры интерпретаций и моделей формальной теории.
45. Опишите синтаксис и семантику языка логики предикатов.
46. Непротиворечивость формализованного исчисления предикатов.
47. Сформулируйте теорему Геделя о неполноте.
48. Дайте определение клаузуальной формы и клаузальной логики.
49. Дайте определение семантической сети. Приведите примеры.
50. Дайте определение клаузы Хорна и ее интерпретации.
51. Опишите метод резолюций для логики предикатов.
52. Опишите принцип логического программирования.
53. Дайте определение конечнозначной логики. Приведите примеры.
54. Дайте определение нечеткой логики. Приведите примеры.
55. Дайте определение модальной логики. Перечислите типы модальностей.
56. Опишите семантику Крипке.

57. Приведите примеры временных (temporальных) логик.
58. Опишите алгоритмическую логику Хоара. Приведите примеры ее использования.
59. Опишите область знаний качественной и количественной теории алгоритмов.
60. Дайте определение алгоритма в виде Машины Тьюринга. Приведите примеры.
61. Дайте определение алгоритма в виде Машины Поста.
62. Сформулируйте тезис Тьюринга - основную гипотезу теории алгоритмов в форме Тьюринга.
63. Дайте определение универсальной машины Тьюринга.
64. Дайте определение универсальной машины Поста.
65. Сформулируйте основную гипотезу теории алгоритмов в форме Маркова.
66. Дайте определение универсального алгоритма Маркова.
67. Перечислите базовые рекурсивные функции. Определите операторы суперпозиции, примитивной рекурсии и минимизации.
68. Дайте определение примитивно рекурсивных функций.
69. Дайте определение частично-рекурсивных функций.
70. Сформулируйте тезис Черча.
71. Дайте определение универсальной частично-рекурсивной функции. Опишите способ ее построения.
72. Приведите примеры алгоритмически неразрешимых задач, невычислимых функций.
73. Что понимается под эффективными алгоритмами?
74. Как оцениваются алгоритмы решения задач?
75. Дайте определение полиномиальной эквивалентности.
76. Дайте определение недетерминированному алгоритму.
77. Опишите недетерминированную машину Тьюринга.
78. Дайте определение классов задач P и NP.
79. Что такое NP – полные задачи?
80. Что такое NP – трудные задачи?
81. Опишите квантовый компьютер.
82. Дайте определение квантовых вычислений.
83. Что такое блоковые коды?
84. Что такое префиксные коды?
85. Как формируется кома-код?
86. Где и как применяется код Грэя?
87. Дайте определение расстояния Хемминга.
88. Приведите примеры кодов, обнаруживающих ошибки.
89. Приведите примеры коды, исправляющие ошибки.
90. Что такое код Хаффмана?
91. Опишите алгоритмы формирования статических и динамических кодов Хаффмана.
92. Дайте определение информационного объема сообщения.
93. Напишите формулу Хартли. Укажите ее области применимости.
94. Напишите формулу Шеннона. Укажите ее области применимости.
95. Дайте определение позиционной системы счисления с натуральным основанием.
96. Опишите алгоритмы выполнения арифметических операций в позиционных системах счисления.
97. Опишите алгоритмы перевода чисел из одной системы счисления в другую.

98. Дайте определение смешанной системы счисления.
99. Приведите примеры нетрадиционных систем счисления: симметричной и ассиметричной.
100. Дайте определение уравновешенной троичной системы счисления.
101. Дайте определение системы счисления с отрицательным основанием.
102. Укажите правила выполнения арифметических операций в негодвоичной системе счисления.
103. Укажите правила выполнения арифметических операций в фибоначчиевой системе счисления.
104. Укажите правила выполнения арифметических операций в факториальной системе счисления.
105. Укажите правила выполнения арифметических операций в системе счисления остаточных классов.
106. Что регламентирует стандарт IEEE 754-2008?
107. Опишите представление целых положительных, отрицательных и беззнаковых чисел в компьютере.
108. Опишите свойства дополнительного кода.
109. Опишите представление вещественных чисел в компьютере.
110. Опишите форматы для представления вещественных чисел со скрытой единицей.
111. Опишите способы представления текстовой информации в компьютере.
112. Опишите способы представления графической информации в компьютере.
113. Опишите способы представления звуковой информации в компьютере.
114. Перечислите методы сжатия информации.
115. Дайте определение абсолютной и относительной погрешности.
116. Опишите источники погрешности при выполнении арифметических операций в компьютере.
117. Опишите аксиоматическое построение множества действительных чисел.
118. Опишите ошибки, связанные с переводом вещественных чисел из десятичной системы в двоичную систему счисления.
119. Опишите ошибки представления чисел в компьютере.
120. Опишите ошибки округления, сдвига и компенсации при выполнении арифметических операций.
121. Опишите основные операции и отношения над множествами.
122. Сформулируйте основные свойства операций алгебры Кантора.
123. Дайте определения сюръективных, инъективных и биективных функций.
124. Определите взаимно однозначное соответствие между двумя заданными множествами.
125. Дайте определения эквивалентности и мощности множеств.
126. Дайте определения счетных и несчетных множеств.
127. Докажите несчетность множества всех бесконечных бинарных последовательностей методом диагонализации Кантора.
128. Дайте определение мощности континуума.
129. Докажите теорему о континуальности множества всех подмножеств множества натуральных чисел.
130. Дайте определения кардинальных чисел, финитных и трансфинитных кардиналов.
131. Сформулируйте теорему Кантора о мощности множества и всех его подмножеств. Опишите шкалу мощностей.
132. Опишите основные свойства операции композиции унарных функций.
133. Опишите свойства бинарных отношений, изоморфизм и гомоморфизм отношений.

134. Определите композицию бинарных отношений, степень отношения, замыкание отношений, ядро отношения.
135. Определите n-арные отношения.
136. Дайте определение частично упорядоченного множества.
137. Опишите алгоритм топологической сортировки вершин графа.
138. Дайте определение отношения эквивалентности на множестве. Сформулируйте аксиомы эквивалентности.
139. Сформулируйте теорему о связи отношениями эквивалентности на множестве и разбиениями этого множества.
140. Определите понятия классов эквивалентности и фактор-множества.
141. Дайте определения графов, мультиграфов, псевдографов, орграфов, гиперграфов и ультраграфов.
142. Дайте определение изоморфизма графов.
143. Приведите способы описания графов в виде матрицы смежности, матрица инциденций, структуры смежности.
144. Дайте определения маршрутов, цепей и циклов.
145. Определите понятия связности, сильной связности и слабой связности в графе.
146. Опишите алгоритм построения компоненты связности, сильной связности и слабой связности.
147. Опишите алгоритм построения точек сочленения.
148. Дайте определения вершинной и реберной связности.
149. Опишите алгоритм построения мостов и блоков.
150. Определите метрические соотношения в графе, приведите аксиомы метрики и метрического пространства.
151. Опишите алгоритмы вычисления расстояния между вершинами графа, радиуса и диаметра графа определения центров графа.
152. Опишите алгоритм поиска выхода из лабиринта.
153. Опишите алгоритмы построения эйлеровых циклов в ориентированном, неориентированном и смешанном графах.
154. Опишите алгоритмы построения гамильтоновых циклов в графе.
155. Опишите алгоритм построения циклов де Брейна.
156. Опишите способы задания волновых графов первого и второго рода (функциональных и контрфункциональных графов) в виде волновой функции.
157. Сформулируйте теорему о характеристических свойствах деревьев и лесов.
158. Опишите алгоритм построения каркаса (остовова).
159. Опишите типы деревьев и способы их задания.
160. Опишите алгоритмы обхода деревьев и способы применения этих алгоритмов.
161. Опишите линейное пространство подграфов заданного графа.
162. Опишите алгоритмы построения фундаментальной системы циклов и разрезов (коциклов).
163. Дайте определение циклического и коциклического ранга графа (цикломатического и коцикломатического числа).
164. Сформулируйте матричную теорему Киркгофа о деревьях.
165. Опишите алгоритмы поиска в глубину и ширину на графе.
166. Опишите алгоритм Краскала построения минимального каркаса взвешенного графа.
167. Опишите алгоритм Прима построения минимального каркаса взвешенного графа.
168. Опишите обобщенный алгоритм Дейкстры в взвешенном графе.

169. Приведите обобщенное уравнение Беллмана-Маслова.
170. Опишите обобщенный алгоритм Флойда-Уоршала.
171. Опишите алгоритм построения совершенного паросочетания двудольного графа.
172. Опишите алгоритм построения системы различных представителей для конечного семейства конечных множеств (трансверсалей).
173. Сформулируйте теорему Холла о совершенных паросочетаниях.
174. Дайте определение сети Петри и ее функционирования.
175. Запишите формулу Эйлера для плоских графов.
176. Сформулируйте критерий планарности графов Понtryгина-Куратовского.
177. Дайте определения хроматического числа и хроматического класса.
178. Сформулируйте теоремы о верхней и нижней оценке хроматического числа.
179. Опишите алгоритм построения внутренне устойчивого множества вершин графа.
180. Опишите алгоритм построения внешне устойчивого множества вершин графа.
181. Опишите алгоритм построения оптимальной раскраски вершин графа.
182. Докажите теорему о пяти красках и сформулируйте теорему о четырех красках.
183. Опишите алгоритм построения максимального потока в многополюсных сетях.
184. Сформулируйте теорему Форда-Фалкерсона о максимальном потоке в сети.
185. Приведите постановку обобщенной задачи о назначениях и обобщенной транспортной задачи.
186. Опишите алгоритмы решения обобщенной задачи о назначениях и обобщенной транспортной задачи.
187. Дайте определения группы, кольца, области целостности и поля.
188. Приведите определения векторного пространства.
189. Сформулируйте теорему Лагранжа о конечной группе и ее подгруппах.
190. Дайте определение матроида, его базы и ранга.
191. Опишите жадный алгоритм на матроидах.
192. Определите сравнимость чисел и полиномов над конечными полями.
193. Опишите алгоритмы построения решета Эратосфена для получения простых чисел и не-приводимых полиномов над конечными полями.
194. Опишите расширенный алгоритм Евклида для вычисления наибольшего общего делителя и наименьшего общего кратного целых чисел и полиномов над конечными полями.
195. Опишите алгоритм решения системы линейных уравнений в конечных кольцах и полях.
196. Сформулируйте китайскую теорему об остатках.
197. Приведите определение функции Мебиуса.
198. Приведите определение и алгоритм вычисления функции Эйлера.
199. Сформулируйте теоремы Эйлера и Ферма.
200. Опишите проблему квадратичного вычета.
201. Опишите проблему дискретного логарифма.
202. Опишите понятие хэш-функции, приведите примеры.
203. Опишите проблему факторизации целых чисел и их тестирования на простоту.
204. Опишите проблему факторизации полиномов над конечным полем.
205. Опишите криптосистему RSA.
206. Опишите числовые и полиномиальные криптосистемы ЭльГамаля.
207. Приведите формулы вычисления числа размещений, перестановок и сочетаний без повторений и с повторениями.
208. Опишите понятие группа подстановок, орбит и стабилизаторов.

209. Опишите алгоритмы описания перестановок, размещений, сочетаний и подмножеств заданного множества.
210. Сформулируйте лемму Бернсайда.
211. Сформулируйте теорема Пойа.
212. Приведите примеры применения теоремы Пойя к решению задач раскраски ожерелий, вершин, ребер и граней многогранников.
213. Опишите основные свойства биномиальных коэффициентов.
214. Дайте определение чисел Стирлинга первого и второго рода.
215. Дайте определение чисел Белла.
216. Сформулируйте принцип включений и исключений.
217. Сформулируйте теоремы о производящих функциях и энумераторах для комбинаторных конфигураций с помощью аппарата формальных степенных рядов.
218. Опишите числовые линейные однородные и неоднородные рекуррентные уравнения.
219. Дайте определение фундаментальной системы решений линейных уравнений.
220. Опишите общее решение линейного рекуррентного уравнения с помощью фундаментальной системы решений.
221. Опишите стационарные линейные рекуррентные уравнения. Дайте определение характеристического полинома и характеристического уравнения.
222. Опишите общее решение однородного и неоднородного стационарного линейного рекуррентного уравнения с помощью фундаментальной системы решений.
223. Опишите алфавитное кодирование и префиксный код.
224. Дайте понятие кодирования с минимальной избыточностью.
225. Опишите алгоритмы сжатия информации Фано и Хаффмена.
226. Дайте определение расстояния Хемминга.
227. Укажите связь Хемминговых сфер с корректирующей способностью.
228. Опишите коды, обнаруживающие и исправляющие ошибки.
229. Приведите описание линейных помехоустойчивых кодов.
230. Опишите алгоритм построения порождающей и проверочной матрицы (генератора и валидатора), а также процесса кодирования и декодирования.
231. Приведите описание циклических кодов.
232. Опишите алгоритм получения порождающего и проверочного полиномов (генератора и валидатора), а также процессы кодирования и декодирования.

9.3 Примеры заданий промежуточного /итогового контроля

Примеры тестовых заданий первого компьютерного теста.

Тестовое задание 1.

Определите правильные ответы. По номерам выбранных ответов сделайте мышкой соответствующие пометки.

Выражение **не** ($|2X - 3Y - 6| \leq 4$) **или** ($|3X + 2Y - 4| \leq 5$) **и** ($4X^2 + Y^2 \leq 16$)

истинно при следующих значениях набора переменных:

1) $X = 1, Y = 3$ 2) $X = 1, Y = -3$ 3) $X = 0, Y = 0$ 4) $X = -1, Y = 0$ 5) $X = -1, Y = 1$

Тестовое задание 2.

Определите правильные ответы. По номерам выбранных ответов сделайте мышкой соответствующие пометки.

Тождественно истинными (тавтологиями) являются логические формулы

- 1) $AB \rightarrow (A + (B \equiv C))$
- 2) $(A \equiv C) \rightarrow (C + \overline{A + B})$
- 3) $(B \equiv C) \rightarrow (C + \overline{AB})$
- 4) $A\overline{BC} \rightarrow (A + B)$
- 5) $BC \rightarrow (A + (B \oplus C))$

Тестовое задание 3.

Решите задание, сравните полученный ответ с предложенными ответами и сделайте мышкой соответствующую пометку.

Корень $X = F(A, B)$ логического уравнения

$$\overline{(A + B)(X \oplus AB)} = \overline{B + \overline{X \rightarrow A}}$$

- 1) $A \rightarrow B$
- 2) $B \rightarrow A$
- 3) $\overline{A \rightarrow B}$
- 4) $\overline{B \rightarrow A}$
- 5) $A \oplus B$

Тестовое задание 4.

Впишите правильный ответ.

Десятичное значение двоичного числа $x_3x_2x_1x_0$, являющегося решением уравнения

$$7x_3 \oplus 14x_2 \oplus 12x_1 \oplus 15x_0 = 6, \text{ равно } \underline{\hspace{2cm}}.$$

Тестовое задание 5.

Решите задание, сравните полученный ответ с предложенными ответами и сделайте мышкой соответствующую пометку.

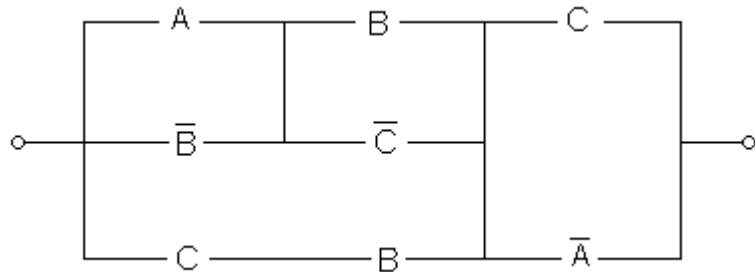
Условие изменения значения логической функции $F(A, B, C) = A(B + C)$ при одновременном изменении аргументов A и B равно

- 1) $(A \oplus B) \rightarrow C$
- 2) $\overline{(A \oplus B) \rightarrow C}$
- 3) $C(A \oplus B)$
- 4) $C \rightarrow (A \oplus B)$
- 5) $\overline{C \rightarrow (A \oplus B)}$

Тестовое задание 6.

Решите задание, сравните полученный ответ с предложенными ответами и сделайте мышкой соответствующую пометку.

Структурная формула для переключательной схемы



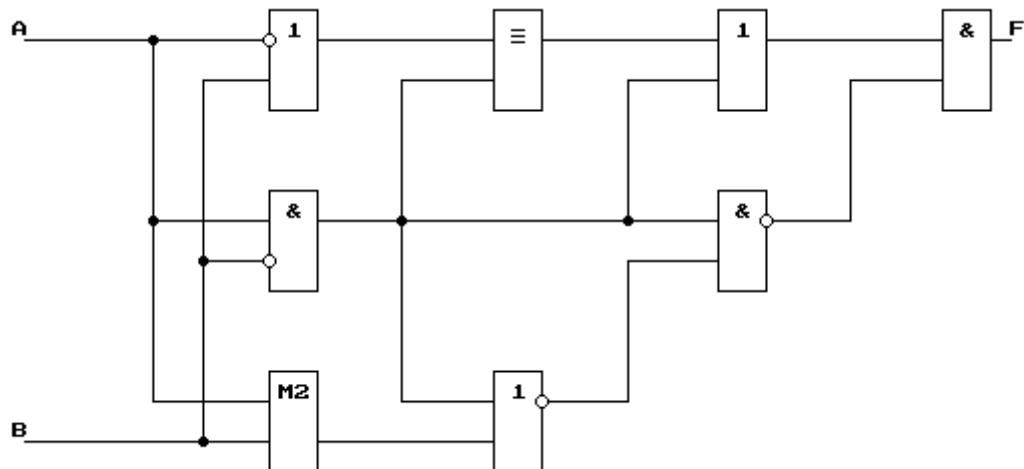
имеет вид

- 1) $(B \rightarrow A)(B \oplus C)$
- 2) $(A \rightarrow B)(B \equiv C)$
- 3) $(B \rightarrow A)(B \equiv C)$
- 4) $(A \rightarrow B)(B \oplus C)$
- 5) $ABC + \bar{A}(B \oplus C)$

Тестовое задание 7.

Решите задание, сравните полученный ответ с предложенными ответами и сделайте мышкой соответствующую пометку.

Комбинационная схема устройства



реализует логическую функцию F равную

- 1) $A \rightarrow B$
- 2) $B \rightarrow A$
- 3) $\overline{A \rightarrow B}$
- 4) $\overline{B \rightarrow A}$
- 5) $A \oplus B$

Тестовое задание 8.

Решите задание, сравните полученный ответ с предложенными ответами и сделайте мышкой соответствующую пометку.

Специализированный компьютер выполняет поразрядные операции над регистрами с именами от A до Z. Машинный язык компьютера содержит следующие команды

Команда	Означает
A?	Ввод данных в регистр A
A!	Вывод данных из регистра A
A*B	Сохранить без изменения единичные разряды регистра A, соответствующие нулевым разрядам регистра B, остальные разряды регистра A инвертировать.

Функция $F(A, B)$, вычисляемая программой

$A?B?F*AA*AF*AF*BB*BA*BF*AF!$

равна

- 1) AB 2) $A \equiv B$ 3) $\overline{A + B}$ 4) $A + B$ 5) $A \oplus B$

Тестовое задание 9.

Решите задание, сравните полученный ответ с предложенными ответами и сделайте мышкой соответствующую пометку.

Три подразделения A, B и C торговой фирмы стремились получить по итогам года прибыль. Экономисты высказали следующие предположения:

- получение прибыли подразделением B не является необходимым условием для получения прибыли подразделением A;
- получение прибыли хотя бы одним из подразделений B или C не является достаточным для получения прибыли подразделением A;
- подразделения A и B не получат прибыль одновременно.

По завершению года оказалось, что только одно из трех предположений истинно.

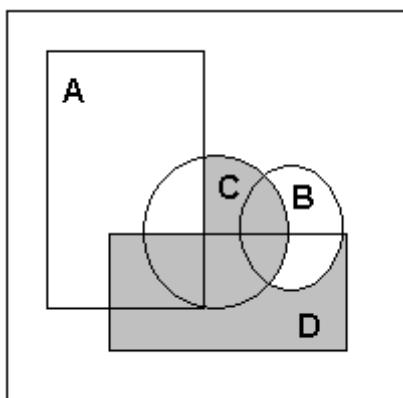
Это означает, что прибыль получили подразделения

- 1) A, C 2) A, B, C 3) A, B 4) B, C 5) C

Тестовое задание 10.

Определите правильные ответы. По номерам выбранных ответов сделайте мышкой соответствующие пометки.

Множество точек выделенной на рисунке области равно



- 1) $(C \cup D)I (C \cup \bar{A})I (D \cup \bar{B})$
 2) $(B \cup C \cup D)I (\bar{A} \cup B \cup D)I (A \cup \bar{B} \cup C)$
 3) $(C \cup D)I (C \cup \bar{B})I (D \cup \bar{A})$
 4) $(B \cup C \cup D)I (A \cup \bar{B} \cup D)I (\bar{A} \cup B \cup C)$
 5) $(C - A) \cup (D - B)$

Тестовое задание 11.

Решите задание, введите ответ с клавиатуры.

Десятичный номер логической функции $F(A, B, C)$ по ее таблице истинности

<i>A</i>	0	0	0	0	1	1	1	1
<i>B</i>	0	0	1	1	0	0	1	1
<i>C</i>	0	1	0	1	0	1	0	1
<i>F</i>	x_7	x_6	x_5	x_4	x_3	x_2	x_1	x_0

вычисляется по формуле $2^7 \cdot x_7 + 2^6 \cdot x_6 + 2^5 \cdot x_5 + 2^4 \cdot x_4 + 2^3 \cdot x_3 + 2^2 \cdot x_2 + 2^1 \cdot x_1 + 2^0 \cdot x_0$.

Десятичный номер логической функции $F(A, B, C)$, заданной системой уравнений

$$\left\{ \begin{array}{l} F(0,1,0)=0 \\ \frac{\partial F}{\partial B}=A \oplus C \\ \frac{\partial F}{\partial(A,C)}=A \equiv C \\ \frac{\partial F}{\partial(B,C)}=B \equiv C \end{array} \right.$$

равен _____.

Тестовое задание 12.

Укажите номера функций, каждая из которых образует базис.

<i>A</i>	<i>B</i>	<i>C</i>	F_1	F_2	F_3	F_4	F_5
0	0	0	1	1	1	1	1
0	0	1	0	0	0	0	1
0	1	0	0	0	0	0	0
0	1	1	0	0	0	1	1
1	0	0	0	0	1	1	0
1	0	1	0	0	1	0	1
1	1	0	0	1	1	0	1
1	1	1	0	0	0	0	0

Тестовое задание 13.

Впишите правильный ответ.

На моторалли выступало 6 гонщиков – Адамс, Брайт, Вест, Гаррисон, Диттер, Эвертон. Пятью болельщиками были высказаны предположения:

- ◆ Первое место займет Адамс, второе – Диттер
- ◆ Первое место будет за Эвертоном, вторым будет Гаррисон
- ◆ Гаррисон будет на третьем месте, а Брайт – на четвертом
- ◆ Брайт будет пятым, а Адамс – вторым
- ◆ Пятым будет Диттер, четвертым Вест

Известно, что в прогнозе каждого болельщика одно утверждение истинное, а другое ложное. Цифры, соответствующие местам, занятым спортсменами, идущими в алфавитном порядке, образуют целое число равное _____.

Тестовое задание 14.

Решите задание, введите ответ с клавиатуры.

Десятичный номер логической функции $F(A, B, C)$ по ее таблице истинности

A	0	0	0	0	1	1	1	1
B	0	0	1	1	0	0	1	1
C	0	1	0	1	0	1	0	1
F	x_7	x_6	x_5	x_4	x_3	x_2	x_1	x_0

вычисляется по формуле $2^7 \cdot x_7 + 2^6 \cdot x_6 + 2^5 \cdot x_5 + 2^4 \cdot x_4 + 2^3 \cdot x_3 + 2^2 \cdot x_2 + 2^1 \cdot x_1 + 2^0 \cdot x_0$.

Логическая функция $F(A, B, C)$ частично задана следующей таблицей истинности

A	0	0	0	0	1	1	1	1
B	0	0	1	1	0	0	1	1
C	0	1	0	1	0	1	0	1
F	1	0	1	-	-	-	1	-

Доопределите частично заданную булеву функцию $F(A, B, C)$ до линейной функции.

Вычислите ее десятичный номер.

Тестовое задание 15.

Решите задание, введите с клавиатуры целое число, цифры которого образуют возрастающую последовательность номеров правильных ответов.

Для бинарного отношения ω , заданного матрицей

$$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

выполняются свойства

- 1) связность $(a \neq b) \Rightarrow (a \omega b) + (b \omega a)$
- 2) рефлексивность $a \omega a$
- 3) антирефлексивность $\overline{a \omega a}$
- 4) симметричность $(a \omega b) \Rightarrow (b \omega a)$
- 5) антисимметричность $(a \omega b) \& (b \omega a) \Rightarrow (a = b)$
- 6) ассиметричность $(a \omega b) \Rightarrow \overline{b \omega a}$
- 7) транзитивность $(a \omega b) \& (b \omega c) \Rightarrow (a \omega c)$

Тестовое задание 16.

Решите задание, введите с клавиатуры целое число, цифры которого образуют возрастающую последовательность номеров правильных ответов.

Для группоида $\langle M, * \rangle$, заданного на множестве $M = \{0, 1, 2\}$ таблицей умножения

*	0	1	2
0	0	1	0
1	1	1	0
2	0	0	2

выполняются свойства

- | | |
|-------------------------------|---|
| 1) ассоциативность | $(a * b) * c = a * (b * c)$ |
| 2) коммутативность | $a * b = b * a$ |
| 3) идемпотентность | $a * a = a$ |
| 4) левый нейтральный элемент | $(\exists e_l \in M)(e_l * a = a)$ |
| 5) правый нейтральный элемент | $(\exists e_r \in M)(a * e_r = a)$ |
| 6) левый поглощающий элемент | $(\exists \infty_l \in M)(\infty_l * a = \infty_l)$ |
| 7) правый поглощающий элемент | $(\exists \infty_r \in M)(a * \infty_r = \infty_r)$ |
| 8) разрешимость уравнения | $a * x = b$ |
| 9) разрешимость уравнения | $x * a = b$ |

Тестовое задание 17.

Решите задание, введите ответ с клавиатуры.

Оператор алгоритмического языка BASIC

PRINT (NOT (15 OR 51) EQV 85) IMP (15 AND 51)

выведет число, равное ____.

Тестовое задание 18.

Решите задание, введите ответ с клавиатуры.

При выполнении нижеследующего оператора,
написанного на языке BASIC, выведено число 14.

PRINT X XOR (X + X)

Исходное значение целочисленной переменной X равно ____.

Тестовое задание 19.

Решите задание, введите ответ с клавиатуры.

Десятичный номер логической функции $F(A, B, C)$ по ее таблице истинности

A	0	0	0	0	1	1	1	1
B	0	0	1	1	0	0	1	1
C	0	1	0	1	0	1	0	1
F	x_7	x_6	x_5	x_4	x_3	x_2	x_1	x_0

вычисляется по формуле $2^7 \cdot x_7 + 2^6 \cdot x_6 + 2^5 \cdot x_5 + 2^4 \cdot x_4 + 2^3 \cdot x_3 + 2^2 \cdot x_2 + 2^1 \cdot x_1 + 2^0 \cdot x_0$.

Десятичный номер производной $\frac{\partial F}{\partial A}$ от функции F , удовлетворяющей системе уравнений

$$\begin{cases} \frac{\partial F}{\partial(B,C)} = A \Rightarrow (B \oplus C) \\ \frac{\partial F}{\partial(A,B,C)} = (A \oplus B) \circ (A \oplus C) \end{cases}$$

равен _____.

Тестовое задание 20.

Решите задание, введите ответ с клавиатуры.

При вычислении кода Грея с помощью оператора,

$G = I \wedge (I >> 1);$

написанного на языке C#,
целочисленной переменной G присвоено значение 48.

Исходное значение целочисленной переменной I равно _____.

Примеры тестовых заданий второго компьютерного теста.

Тестовое задание 1.

Решите задание, введите ответ с клавиатуры.

Результат применения машины Тьюринга

		alfabet	
		0	1
s	A	_ 1 B	0 r A
t	B	_ s B	_ 1 B
a	C	_ s C	0 1 C
t	D	1 1 C	1 1 D
e	E	0 1 D	0 1 E

к входному слову 1000 равен _____.

Тестовое задание 2.

Решите задание, введите ответ с клавиатуры.

В результате работы машины Тьюринга

		alfabet	
		0	1
s	A	— 1 B	0 r A
t	B	— s B	1 1 B
a	C	— s C	0 1 C
t	D	1 1 C	1 1 D
e	E	0 1 D	0 1 E
		0 1 E	1 1 E

получено выходное слово 100111. Входное слово минимальной длины равно _____.

Тестовое задание 3.

Решите задание, введите ответ с клавиатуры.

Результат применения нормального алгоритма Маркова

```

A0->0A
A1->1A
A->B
0B->B
1B->E0
B!->
0C->C0
1C->D1
C!->
0D->C1
1D->E0
D!->1
0E->D0
1E->E1
E!->10
->A

```

к входному слову 1000 равен _____.

Тестовое задание 4.

Решите задание, введите ответ с клавиатуры.

В результате работы нормального алгоритма Маркова

```

A0->0A
A1->1A
A->B
0B->B1
1B->E0
B!->
0C->C0
1C->D1
C!->
0D->C1
1D->E0
D!->1
0E->D0
1E->E1
E!->10
->A

```

получено выходное слово 100111. Входное слово минимальной длины равно _____.

Тестовое задание 5.

Решите задание, введите ответ с клавиатуры.

Значение функции F(19)

```
A=S<N,I[3,3]>;
B=R<I[1,1],A>;
C=S<B,I[1,1],I[1,1]>;
D=S<B,C,I[1,1]>;
F=S<N,D>;
```

равно ____.

Тестовое задание 6.

Решите задание, введите ответ с клавиатуры.

Если значение функции F(X)

```
A=S<N,I[2,3]>;
B=R<I[1,1],A>;
C=S<B,I[1,1],I[1,1]>;
D=S<B,C,I[1,1]>;
F=S<N,D>;
```

равно 20, то значение аргумента X равно ____.

Тестовое задание 7.

Решите задание, введите ответ с клавиатуры.

В результате выполнения программы

```
using System;
class RF
{
    static int F(int X)
    {
        return X==1 ? 0 : X%2==1 ? 2*F((X-1)/2)+1 : 2*F(X/2)+2;
    }
    static void Main()
    {
        Console.WriteLine(F(17));
    }
}
```

будет выведено число, равное ____.

Тестовое задание 8.

Решите задание, введите ответ с клавиатуры.

В результате выполнения программы

```
using System;
class RF {
    static string F(int i, int n)
    {
        return i > n ? "" : F(2 * i, n) + i.ToString() + F(2 * i + 1, n);
    }
    static void Main()
    {
        Console.WriteLine(F(1, 9));
    }
}
```

будет выведена строка, равная ____.

Тестовое задание 9.

Определите правильные ответы. По номерам выбранных ответов сделайте мышкой соответствующие пометки.

Функция F

```
using System;
class RF
{
    static string F(string X)
    {
        if (X.Length > 1)
        {
            string T = X.Substring(1);
            switch (X.Substring(0, 1))
            {
                case "0": return T;
                case "1": return F(T) + '0' + F(T);
                default: return F(X);
            }
        }
        else return F(X);
    }
    static void Main()
    {
        Console.Write("X=");
        Console.WriteLine("F(X)=" + F(Console.ReadLine()));
    }
}
```

применима к следующим входным словам

- 1) 0111 2) 1110 3) 1101 4) 1021 5) 1201

Тестовое задание 10.

Решите задание, введите ответ с клавиатуры.

Следующая программа выводит результат вычисления функции F

```
using System;
class RF
{
    static string F(string X)
    {
        if (X.Length > 1)
        {
            string T = X.Substring(1);
            switch (X.Substring(0, 1))
            {
                case "0": return T;
                case "1": return F(T) + '0' + F(T);
                default: return F(X);
            }
        }
        else return F(X);
    }
    static void Main()
    {
        Console.Write("X=");
        Console.WriteLine("F(X)=" + F(Console.ReadLine()));
    }
}
```

Строка X, для которой F(X)=X, равна ____.

Тестовое задание 11.

Решите задание, сравните полученный ответ с предложенными ответами и сделайте мышкой соответствующую пометку.

Восьмеричное число $0.3(52)_8$ в системе счисления по основанию 16 равно

- 1) $0.7(A)_{16}$ 2) $0.3(A)_{16}$ 3) $0.3(A2)_{16}$ 4) $0.7(5)_{16}$ 5) $0.3(2A)_{16}$

Тестовое задание 12.

Решите задание, введите ответ с клавиатуры.

Алфавит племени Пиджен состоит из четырех букв. Аборигены закодировали слово DABC с использованием следующей кодовой таблицы:

A	B	C	D
0	1	01	10

и передали его, не сделав промежутков, отделяющих одну букву от другой. Количество способов прочтения переданного слова равно ____.

Тестовое задание 13.

Решите задание, введите ответ с клавиатуры. Если в ответе получается число в виде дроби, то округлите его до целого числа. Ответом может быть только целое число.

В княжестве Блэквайтия имеются автомобили только черного, серого и белого цвета. Информационный объем сообщения "В аварию попал автомобиль не черного цвета" равен $8 - \log_2 5$ бит. Количество информации, содержащееся в сообщении "В аварию попал серый автомобиль", равно 8 бит. Количество бит информации в сообщении "В аварию попал автомобиль белого цвета" равно ____.

Тестовое задание 14.

Решите задание, введите ответ с клавиатуры. Для записи цифр превышающих 9 используйте заглавные латинские буквы.

Трехзначное число, записанное в шестнадцатеричной системе счисления, увеличивается вдвое от перестановки первой цифры в конец числа. Максимальное из таких чисел, записанное в системе счисления по основанию 16, равно ____.

Тестовое задание 15.

Решите задание, введите ответ с клавиатуры. Для записи цифр превышающих 9 используйте заглавные латинские буквы.

Вторая цифра шестнадцатеричного четырехзначного числа равна 5. Первую цифру переставили в конец числа. Полученное число оказалось на 3F1B16 меньше исходного. Исходное число, записанное в системе счисления по основанию 16, равно ____.

Тестовое задание 16.

Решите задание, введите ответ с клавиатуры.

Наименьшее основание позиционной системы счисления x , при котором $104_x = 555_y$, равно ____.

Тестовое задание 17.

Решите задание, введите ответ с клавиатуры.

Переменные X, X1, X2, X3 имеют размер – байт, тип – знаковый. В шестнадцатеричной системе счисления X1=C1₁₆, X2=DB₁₆, X3=C5₁₆. Значение выражения X=(X1-X2)*X3 в десятичной системе счисления равно ____.

Тестовое задание 18.

Решите задание, введите ответ с клавиатуры. Если в ответе получается число в виде дроби, то округлите его до целого числа. Ответом может быть только целое число.

Значение переменной A представлено в формате с плавающей точкой в шестнадцатеричной системе счисления $A=C2F20000_{16}$. Тип переменной A – single для языков BASIC и PASCAL. Десятичное значение числа A равно ____.

Тестовое задание 19.

Решите задание, введите ответ с клавиатуры. При записи числа используйте точку в качестве разделителя целой и дробной частей. Период заключайте в круглые скобки. Для записи цифр больших девятери используйте заглавные латинские буквы. В записи числа указывать основание системы счисления не нужно.

Число $X=121.(123321)$ записано в виде периодической дроби в системе счисления по основанию 5. Здесь в скобках указан период дроби. Число X, записанное в виде периодической дроби в системе счисления по основанию 7, равно _____.

Тестовое задание 20.

Решите задание, введите ответ с клавиатуры.

Число различных наборов значений логических переменных $x_1, x_2, \dots, x_9, x_{10}$, которые удовлетворяют системе логических уравнений

$$\left\{ \begin{array}{l} x_1 + x_2 \cdot x_3 = 1 \\ x_2 + x_3 \cdot x_4 = 1 \\ \dots \\ x_7 + x_8 \cdot x_9 = 1 \\ x_8 + x_9 \cdot x_{10} = 1 \end{array} \right.$$

равно _____.

Примеры тестовых заданий третьего компьютерного теста.

Тестовое задание 1.

Решите задание, введите ответ с клавиатуры.

Граф $G = \langle V, E \rangle$, где $V = \{1, 2, 3, 4\}$, задан весовой матрицей смежности

0	1	7	9
1	0	6	8
7	6	0	6
9	8	6	0

Вес наименьшего (кратчайшего) связывающего дерева равен _____.

Тестовое задание 2.

Решите задание, введите ответ с клавиатуры.

Граф $G = \langle V, E \rangle$, где $V = \{1,2,3,4\}$, задан матрицей смежности

0	1	1	1
1	0	0	0
1	0	0	0
1	0	0	0

Диаметр графа равен ____.

Тестовое задание 3.

Решите задание, введите ответ с клавиатуры.

Граф $G = \langle V, E \rangle$, где $V = \{1,2,3,4\}$, задан волновой функцией $W: V \rightarrow V \cup \{0\}$.
Здесь $E = \{(W(I), I) | I \in V \text{ & } W(I) \neq 0\}$.

I	1	2	3	4
W	3	4	1	0

Количество компонент связности в графе равно ____.

Тестовое задание 4.

Решите задание, введите ответ с клавиатуры.

Граф $G = \langle V, E \rangle$, где $V = \{1,2,3,4\}$, задан матрицей смежности

0	0	0	1
0	0	1	1
0	1	0	0
1	1	0	0

Цифры кода Прюфера для данного графа образуют целое число, равное ____.

Тестовое задание 5.

Определите правильные ответы.

По номерам выбранных ответов сделайте мышкой соответствующие пометки.

Отношение эквивалентности, определенное на множестве из 3 элементов, содержит n пар, при n , равном:

- 1) 1 2) 2 3) 3 4) 4 5) 5

Тестовое задание 6.

Решите задание, введите ответ в виде числа с клавиатуры.

Граф $G = \langle V, E \rangle$, где $V = \{1,2,3,4\}$, задан весовой матрицей смежности

	3	9	
		1	6

Кратчайшее расстояние между вершинами 1 и 4 равно ____.

Тестовое задание 7.

Решите задание, введите ответ в виде числа с клавиатуры.

Дерево, построенное на 16 вершинах, имеет 11 вершин степени 2.

Остальные вершины либо листья, либо вершины степени 4.

Число листьев в дереве равно ____.

Тестовое задание 8.

Решите задание, введите ответ в виде числа с клавиатуры.

В плоском графе, считая внешнюю грань, десять граней: три треугольника, пять четырехугольников, по одному пятиугольнику и шестиугольнику.

Висячих вершин в этом графе нет. Количество вершин графа равно ____.

Тестовое задание 9.

Решите задание, введите ответ в виде числа с клавиатуры.

Граф $G = \langle V, E \rangle$, где $V = \{1,2,3\}$, задан матрицей смежности

0	1	1
1	0	1
1	1	0

Число каркасов графа равно ____.

Тестовое задание 10.

Определите правильные ответы.

По номерам выбранных ответов сделайте мышкой соответствующие пометки.

Граф $G = \langle V, E \rangle$, где $V = \{1,2,3,4,5\}$, задан матрицей смежности

0	1	0	1	1
1	0	0	1	0
1	1	0	0	1
1	1	0	0	0
0	0	0	1	0

Укажите максимальные внутренне устойчивые множества графа

- 1) {1} 2) {2} 3) {2,5} 4) {3,4} 5) {1,2,5}

Тестовое задание 11.

Решите задание, введите ответ в виде числа с клавиатуры.

Граф $G = \langle V, E \rangle$, где $V = \{1,2,3,4\}$, задан матрицей смежности

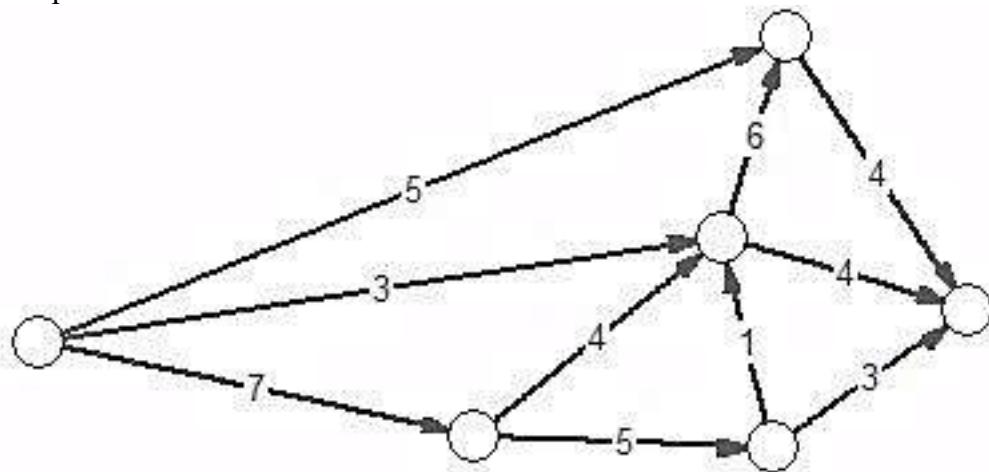
0	0	0	0
0	0	0	1
0	0	0	1
0	1	1	0

Цикломатическое число графа равно ____.

Тестовое задание 12.

Решите задание, введите ответ в виде числа с клавиатуры.

Для транспортной сети



величина максимального потока равна ____.

Тестовое задание 13.

Определите правильные ответы. По номерам выбранных ответов сделайте мышкой соответствующие пометки.

Двудольный граф $G = \langle X \cup Y, E \rangle$, где $X = \{x_1, x_2, x_3, x_4, x_5, x_6\}$, $Y = \{y_1, y_2, y_3, y_4, y_5, y_6\}$, $E \subset X \times Y$, задан матрицей смежности

0	0	0	1	0	1
0	0	0	0	1	0
0	0	0	1	1	1
1	0	1	0	0	0
0	1	1	0	0	0
1	0	1	0	0	0

Укажите максимальные паросочетания двудольного графа.

- 1) $\{(x_1, y_4), (x_2, y_5), (x_3, y_6)\}$
- 2) $\{(x_1, y_6), (x_3, y_4), (x_2, y_5)\}$
- 3) $\{(x_1, y_4), (x_2, y_5), \}$
- 4) $\{(x_2, y_5), (x_3, y_6)\}$
- 5) $\{(x_3, y_4), (x_2, y_5)\}$

Тестовое задание 14.

Решите задание, введите ответ в виде числа с клавиатуры.

В плоском графе четыре вершины. Все четыре грани графа, считая внешнюю грань, являются n -угольниками. Висячих вершин в этом графе нет. Число n равно ____.

Тестовое задание 15.

Решите задание, введите ответ в виде числа с клавиатуры.

Коммерческий университет арендует здание для проведения занятий. В четверг должны быть прочитаны 4 лекции, по одной для каждого из следующих предметов: дискретная математика (ДМ), английский язык (АЯ), программирование (П), математический анализ (МА). Время чтения каждой лекции – два академических часа. Лекции, читаемые одним преподавателем, или имеющиеся в рабочем учебном плане студентов не могут стоять в расписании в одинаковое время. В таблице знаком «+» отмечены лекции, которые не могут читаться одновременно.

	ДМ	АЯ	П	МА
ДМ		+	+	+
АЯ	+		+	
П	+	+		+
МА	+		+	

Минимальное количество академических часов, за которое могут быть прочитаны лекции в четверг, равно _____.

Тестовое задание 16.

Решите задание, введите ответ в виде числа с клавиатуры.

Граф $G = \langle V, E \rangle$, где $V = \{1, 2, 3, 4\}$, задан весовой матрицей смежности

0	10	6	36
10	0	15	5
6	15	0	35
36	5	35	0

Код дерева путей $T = \langle V, E_T \rangle$, где $E_T \subset E$, задается целым числом, образованным последовательностью цифр $w_1 w_2 w_3 w_4$ волновой функции $W: V \rightarrow V \cup \{0\}$:

i	1	2	3	4
W	w_1	w_2	w_3	w_4

Здесь $E_T = \{(w_i, i) | i \in V \text{ & } w_i \neq 0\}$, а вершина $i \in V$, для которой $w_i = 0$, является корнем дерева.

Тестовое задание 17.

Решите задание, введите ответ в виде числа с клавиатуры.

В классе каждый мальчик дружит ровно с четырьмя девочками, а каждая девочка – ровно с тремя мальчиками. В классе 16 парт, а на последней экскурсии было 23 школьника. Количество учеников в классе равно _____.

Тестовое задание 18.

Решите задание, введите ответ в виде числа с клавиатуры.

Маша и Катя пошли в тир. Уговор был такой: каждая из девушек по отдельности делает 2 выстрела и за каждое попадание получает право ещё на два выстрела. Маша выстрелила 4 раза, а Катя – 6. Суммарное количество попаданий, которое совершили девушки, стреляя по отдельности, равно _____.

Тестовое задание 19.

Решите задание, введите ответ в виде числа с клавиатуры.

Город имеет форму квадрата 20 на 20 метров с 3 прямолинейными улицами, идущими параллельно одной стороне квадрата, и 3 прямолинейными улицами, идущими параллельно другой стороне. Расстояние между любыми двумя соседними параллельными улицами – 10 метров, длина каждой улицы – 20 метров. Мэр города решил выполнить свое предвыборное обещание: заасфальтировать за свой счет улицы так, чтобы с любого перекрестка на любой другой можно было проехать по асфальту. Конечно, мэр хочет истратить как можно меньше своих денег. Минимальная длина улиц, которые мэр может покрыть асфальтом, равна ____.

Тестовое задание 20.

Решите задание, введите ответ в виде числа с клавиатуры.

В стране 7 озер, соединенных между собой 11 каналами, причем от любого озера можно доплыть до любого другого. Количество островов, образованных озерами и каналами равно ____.

Примеры тестовых заданий четвертого компьютерного теста.

Тестовое задание 1.

Решите задание, введите ответ в виде числа с клавиатуры.

Передано двоичное сообщение $a_0a_1a_2a_3$, закодированное словом $b_0b_1b_2b_3b_4b_5b_6$ в алфавите $B = \{0,1\}$. Символы $b_0b_1b_2b_3b_4b_5b_6$ являются коэффициентами булевого полинома $B(x) = b_0 + b_1x + b_2x^2 + b_3x^3 + b_4x^4 + b_5x^5 + b_6x^6$, вычисляемого по формуле $B(x) = A(x) \cdot x^3 + A(x) \cdot x^3 \bmod(1 + x + x^3)$, где $A(x) = a_0 + a_1x + a_2x^2 + a_3x^3$ - булев полином, соответствующий исходному сообщению $a_0a_1a_2a_3$. Известно, что при передаче сообщения полученное слово $b_0b_1b_2b_3b_4b_5b_6$ могло быть искажено одиночной ошибкой. Для полученного слова 0111100 исходное двоичное сообщение равно ____.

Тестовое задание 2.

Решите задание, введите ответ в виде числа с клавиатуры.

Передано двоичное сообщение $a_0a_1a_2a_3$, закодированное словом $b_0b_1b_2b_3b_4b_5b_6$ в алфавите $B = \{0,1\}$. Символы $b_0b_1b_2b_3b_4b_5b_6$ являются коэффициентами булевого полинома $B(x) = b_0 + b_1x + b_2x^2 + b_3x^3 + b_4x^4 + b_5x^5 + b_6x^6$, вычисляемого по формуле $B(x) = A(x) \cdot x^3 + A(x) \cdot x^3 \bmod(1 + x + x^3)$, где $A(x) = a_0 + a_1x + a_2x^2 + a_3x^3$ - булев полином, соответствующий исходному сообщению $a_0a_1a_2a_3$. Известно, что при передаче сообщения полученное слово $b_0b_1b_2b_3b_4b_5b_6$ искажено одиночной ошибкой. Для полученного слова 0111100 номер искаженного бита равен ____.

Тестовое задание 3.

Решите задание, введите ответ в виде числа с клавиатуры.

Передано двоичное сообщение $a_0a_1a_2a_3$, закодированное словом $b_0b_1b_2b_3b_4b_5b_6$ в алфавите

$B = \{0,1\}$. Символы $b_0b_1b_2b_3b_4b_5b_6$ являются коэффициентами булевого полинома

$B(x) = b_0 + b_1x + b_2x^2 + b_3x^3 + b_4x^4 + b_5x^5 + b_6x^6$, вычисляемого по формуле

$B(x) = A(x) \cdot (1 + x + x^3)$, где $A(x) = a_0 + a_1x + a_2x^2 + a_3x^3$ - булев полином, соответствующий исходному сообщению $a_0a_1a_2a_3$. Известно, что при передаче сообщения полученное слово $b_0b_1b_2b_3b_4b_5b_6$ могло быть искажено одиночной ошибкой. Для полученного слова 0111100 исходное двоичное сообщение равно _____.

Тестовое задание 4.

Решите задание, введите ответ в виде числа с клавиатуры.

Передано двоичное сообщение $a_0a_1a_2a_3$, закодированное словом $b_0b_1b_2b_3b_4b_5b_6$ в алфавите

$B = \{0,1\}$. Символы $b_0b_1b_2b_3b_4b_5b_6$ являются коэффициентами булевого полинома

$B(x) = b_0 + b_1x + b_2x^2 + b_3x^3 + b_4x^4 + b_5x^5 + b_6x^6$, вычисляемого по формуле

$B(x) = A(x) \cdot (1 + x + x^3)$, где $A(x) = a_0 + a_1x + a_2x^2 + a_3x^3$ - булев полином, соответствующий исходному сообщению $a_0a_1a_2a_3$. Известно, что при передаче сообщения полученное слово $b_0b_1b_2b_3b_4b_5b_6$ искажено одиночной ошибкой. Для полученного слова 0111100 номер искаженного бита равен _____.

Тестовое задание 5.

Решите задание, введите ответ в виде числа с клавиатуры.

Число бит, на которое уменьшится код заключенного в кавычки сообщения «ЕНОТ НЕ ТОНЕТ», сжатого алгоритмом Хаффмана, по сравнению с оптимальным равномерным кодированием равно _____.

Тестовое задание 6.

Решите задание, введите ответ с клавиатуры.

Значение переменной C, вычисленное в программе, написанной на языке Pascal,

```

var K,C:integer;
begin
  C:=0;
  for K:=1 to 1000 do
    if (K mod 30 = 0) or (K mod 42 = 0) or (K mod 70 = 0) then C:=C+1;
    writeln('C=',C)
  end.

```

равно _____.

Тестовое задание 7.

Решите задание, введите ответ с клавиатуры.

База данных "Врачи", наряду с другими, имеет поля с названиями "пол" и "специальность". В базе данных находятся записи о врачах трех специальностей. Количество записей N, удовлетворяющих различным запросам, приведено в следующей таблице

ЗАПРОС	N
пол=м или специальность≠хирург	33
неверно, что (пол=ж или специальность=окулист)	11
пол=м и специальность=терапевт	5

Количество записей, удовлетворяющих запросу "специальность≠хирург", равно ____.

Тестовое задание 8.

Решите задание, введите ответ с клавиатуры.

В результате работы программы

```
using System;
class Test
{
    static void Main()
    {
        Console.Write("X=");
        byte X = byte.Parse(Console.ReadLine());
        byte Y = 5;
        byte Z =(byte)(X * Y);
        Console.WriteLine("Z=" + Z.ToString());
        Console.ReadLine();
    }
}
```

На консоль выведена строка Z=7.

Введенное значение X равно ____.

Тестовое задание 9.

Решите задание, введите ответ с клавиатуры.

В результате работы программы

```
using System;
class Test
{
    static void Main()
    {
        Console.Write("X=");
        sbyte X = sbyte.Parse(Console.ReadLine());
        sbyte Y = 5;
        sbyte Z =(sbyte)(X * Y);
        Console.WriteLine("Z=" + Z.ToString());
        Console.ReadLine();
    }
}
```

На консоль выведена строка Z=7

Введенное значение X равно ____.

Тестовое задание 10.

Решите задание, введите ответ в виде числа с клавиатуры.

Количество решений в целых числах уравнения $X_1 + X_2 + X_3 + X_4 = 30$

при дополнительных ограничениях $X_1 \geq 1, X_2 \geq -5, X_3 \geq 0, X_4 \geq 8$ равно ____.

Тестовое задание 11.

Решите задание, введите ответ в виде числа с клавиатуры.

Имеются две колоды из 6 карт каждая. Карты, содержащиеся в каждой колоде, одинаковые. В первой колоде фиксирован порядок карт. Количество способов, которыми можно уложить карты во второй колоде таким образом, чтобы при одновременном открывании верхних карт обеих колод, получилось ровно 4 совпадения, равно ____.

Тестовое задание 12.

Решите задание, введите ответ в виде числа с клавиатуры.

Ожерелья, получающиеся передвижением бусинок по нитке ожерелья, а также переворотом ожерелья, считаются одинаковыми. Количество различных ожерелий из 7 бусинок, которые можно составить, используя 3 красных и 4 синих бусинки, равно ____.

Тестовое задание 13.

Решите задание, введите ответ в виде числа с клавиатуры.

Десятичный код $K(B)$ полинома $B(x) = b_n x^n \oplus b_{n-1} x^{n-1} \oplus K \oplus b_2 x^2 \oplus b_1 x \oplus b_0$ из кольца $\mathbf{Z}_2[x]$ вычисляется по формуле $K(B) = b_n \cdot 2^n + b_{n-1} \cdot 2^{n-1} + K + b_2 \cdot 2^2 + b_1 \cdot 2 + b_0$.

Полиномы $A(x)$ и $B(x)$ из кольца $\mathbf{Z}_2[x]$ заданы своими десятичными кодами

$K(A) = 753$ и $K(B) = 969$. Десятичный код $K(C)$ полинома $C(x) = HOD(A(x), B(x))$ равен ____.

Тестовое задание 14.

Решите задание, введите ответ в виде числа с клавиатуры.

Десятичный код $K(B)$ полинома $B(x) = b_n x^n \oplus b_{n-1} x^{n-1} \oplus K \oplus b_2 x^2 \oplus b_1 x \oplus b_0$ из кольца $\mathbf{Z}_2[x]$ вычисляется по формуле $K(B) = b_n \cdot 2^n + b_{n-1} \cdot 2^{n-1} + K + b_2 \cdot 2^2 + b_1 \cdot 2 + b_0$.

Десятичный код $K(B)$ полинома $B(x)$, удовлетворяющего уравнению

$((x^4 \oplus x + 1) \cdot B(x) = (x^3 \oplus x \oplus 1)) \bmod (x^7 \oplus x \oplus 1)$ равен ____.

Тестовое задание 15.

Решите задание, введите ответ с клавиатуры.

В результате работы программы

```
using System;
class Test
{
    static void Main()
    {
        int[] m = { 7, 11, 13 };
        Console.WriteLine("X=");
        int X = int.Parse(Console.ReadLine());
        if ((0 <= X) && (X < m[0] * m[1] * m[2]))
            for(int i=0;i<m.Length;i++) Console.Write(X % m[i]);
        Console.ReadLine();
    }
}
```

На консоль выведена строка 5910.

Введенное значение X равно ____.

Тестовое задание 16.

Решите задание, введите ответ в виде числа с клавиатуры.

На интерпретациях из двух предметов s и t код предиката R определяется строкой бит $abcd$, где $a = R(s, s)$, $b = R(s, t)$, $c = R(t, s)$, $d = R(t, t)$.

Определите количество k предикатов и минимальный в лексикографическом порядке код предиката R , для которых формула $\forall y R(y, y) \Rightarrow \forall x \exists y R(x, y)$ опровергима.

Ответ укажите в виде строки символов $kabcd$.

Если таких предикатов нет, укажите в качестве ответа символ 0.

Тестовое задание 17.

Решите задание, введите ответ в виде числа с клавиатуры.

Целые числа A и B принадлежат отрезку $[1, 96]$.

Количество пар чисел A и B , для которых сравнение $A \cdot X \equiv B \pmod{97}$ однозначно разрешимо относительно переменной X равно ____.

Тестовое задание 18.

Решите задание, введите ответ в виде числа с клавиатуры.

Корень x уравнения $17 \cdot C_{2x-1}^x = 9 \cdot C_{2x}^{x-1}$ равен ____.

Тестовое задание 19.

Решите задание, введите ответ в виде числа с клавиатуры.

Число решений в натуральных числах уравнения $x^2 \cdot y^3 = 2^6 \cdot 3^7$ равно ____.

Тестовое задание 20.

Решите задание, введите ответ в виде числа с клавиатуры.

Анаграммой называется произвольное слово, полученное из данного слова перестановкой букв.

Количество анаграмм, которые можно получить из слова «ПЕРЕШЕЕК», равно ____.

В стране 7 озер, соединенных между собой 11 каналами, причем от любого озера можно доплыть до любого другого. Количество островов, образованных озерами и каналами равно ____.

10 Учебно-методическое и информационное обеспечение дисциплины

10.1 Базовые учебники

- **Авдошин С.М., Набебин А.А.** Дискретная математика. Модулярная алгебра, криптография, кодирование. – М.: ДМК Пресс, 2017. – 352 с.
- **Андерсон Дж.** Дискретная математика и комбинаторика. М.: Вильямс, 2004. – 960 с.

10.2 Основная литература

- **Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В.** Основы криптографии: Учебное пособие, 2-е изд., испр. и доп. М.: "Гелиос АРВ", 2002. 480 с.
- **Андреева Е.В., Босова Л.Л., Фалина И.Н.** Математические основы информатики. М.: Бином, 2007. – 328 с.
- **Гринченков Д.В., Потоцкий С.И.** Математическая логика и теория алгоритмов для программистов. М.: КНОРУС, 2014. – 206 с.
- **Колмогоров А.Н., Драгалин А.Г.** Математическая логика. Введение в математическую логику. Едиториал УРСС, 2013. – 240.
- **Кузнецов О.П.** Дискретная математика для инженеров. Книга по требованию, 2012. – 410 с.
- **Липский В.** Комбинаторика для программистов. Книга по требованию, 2012. – 200 стр.
- **Набебин А.А.** Дискретная математика. Научный мир, 2010. – 512 с.
- **Новиков Ф.А.** Дискретная математика для программистов. СПб.: Питер, 2012. – 400 с.
- **Хаггард Г., Шлифф Дж., Уайтрайд С.** Дискретная математика для программистов. М.: БИНОМ. Лаборатория знаний, 2013. – 627 с.
- **Хаггарти Р.** Дискретная математика для программистов. Техносфера, 2012. – 400 с.

10.3 Дополнительная литература

- **Абрамов С.А.** Лекции о сложности алгоритмов. МЦНМО, 2012. – 248 с.
- **Алексеев В.Б.** Лекции по дискретной математике. М.: Изд. отд. Фак. ВМиК МГУ им. М.В.Ломоносова, 2004. 74 с.
- **Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В.** Основы криптографии: Учебное пособие, 2-е изд., испр. и доп. М.: "Гелиос АРВ", 2002. 480с
- **Ахо А., Ульман Дж.** Теория синтаксического анализа, перевода и компиляции. Том 1, М.: Мир, 1978. 613с. Том 2, М.: Мир, 1978. 488с.
- **Берлекэмп Э.** Алгебраическая теория кодирования. М.: МИР, 1971. 250 с.
- **Биркгоф Г.** Теория решеток. М.: Наука, 1984. - 568 с.
- **Биркгоф Г., Барти Т.** Современная прикладная алгебра. М.: Мир, 1976. - 400 с.
- **Босс В.** Лекции по математике. Т. 6: Алгоритмы, логика, вычислимость. От Диофанта до Тьюринга и Геделя. Либроком, УРСС, 2012. – 2008 с.
- **Брайант Р., О'Халларон Д.** Компьютерные системы: архитектура и программиование. СПб.: БХВ-Петербург, 2005. – 1104 с.
- **Верещагин Н.К., Шень А.** Начала теории множеств. МЦНМО, 2012. – 112 с.
- **Верещагин Н.К., Шень А.** Языки и исчисления. МЦНМО, 2012. – 240 с.
- **Верещагин Н.К., Шень А.** Вычислимые функции. МЦНМО, 2012. – 160 с.

- Гаврилов Г.П., Сапоженко А.А. Сборник задач по дискретной математике. М.: Наука, 1977. - 368с.
- Горбатов В.В. Фундаментальные основы дискретной математики. М.: Наука, Физматлит, 1999.
- Гуц А.К. Математическая логика и теория алгоритмов. Либерком, 2009. – 120 с.
- Зыков А.А. Основы теории графов. М.: Наука, 1987. 384 с.
- Калужнин Л.А., Сущанский В.И. Преобразования и перестановки. М.: Наука, 1985. - 160 с.
- Клини С.К. Введение в метаматематику. М.: Либроком, 2008. – 526 с.
- Клини С.К. Математическая логика. М.: ЛКИ, 2008. – 482 с.
- Кон П. Универсальная алгебра. М.: Мир, 1968. - 352 с.
- Кофман А. Введение в прикладную комбинаторику. М.: Наука, 1975. 480 с.
- Кристофиес Н. Теория графов: алгоритмический подход. М.: МИР, 1978. 430с.
- Кузнецов О.П., Адельсон-Вельский Г.М. Дискретная математика для инженера. М.: Энергоатомиздат, 1988. 480с.
- Лавров И.А. Математическая логика. М.: Академия, 2006. – 240 с.
- Лавров И.А., Максимова Л.Л. Задачи по теории множеств, математической логике и теории алгоритмов. М.: Физматлит, 2004. – 256 с.
- Ландо С.К. Введение в дискретную математику. МЦНМО, 2012. – 272 с.
- Лидл Р., Нидеррайтер Г. Конечные поля. М.: Мир, 1988. - 820 с.
- Липский В. Комбинаторика для программистов. М.: Мир, 1988. - 213 с.
- Локшин А.А., Сагомонян Е.А. Логика и множества. М.: “Вузовская книга”, 2002. – 64 с.
- Мальцев А.И. Алгоритмы и рекурсивные функции. М.: Наука, Физматлит, 1986. – 392 с.
- Мендельсон Э. Введение в математическую логику. М.: Либроком, 2010. – 161 с.
- Набебин А.А. Сборник заданий по дискретной математике. Научный мир, 2009. – 280 с.
- Набебин А.А., Кораблин Ю.П. Математическая логика и теория алгоритмов. Научный мир, 2008. – 344 с.
- Набебин А.А. Логика и Пролог в дискретной математике. М.: Изд-во МЭИ, 1996. 452 с.
- Непейвода Н.Н. Прикладная логика. – Новосибирск, НГУ, 2000. - 494 с.
- Новиков Ф.А. Дискретная математика. Питер, 2012. – 400 с.
- Питерсон У. Коды, исправляющие ошибки. М.: Мир, 1964. 339с.
- Риордан Дж. Введение в комбинаторный анализ. М.: ИЛ, 1963. 288 с.
- Романовский И.В. Дискретный анализ. БХВ-Петербург, 2008. – 336 с.
- Рыбников К.А. Введение в комбинаторный анализ. М.: Изд-во Моск. ун-та. 1985. 308 с.
- Смолин Ю.Н. Числовые системы. Флинта, Наука. -2009. – 112 с.
- Уилсон Р. Введение в теорию графов. М.: Мир, 1977. - 208 с.
- Черч А. Введение в математическую логику. Том 1. Либроком, 2009. – 482 с.
- Хаггарти Р., Шлипф Дж., Уайтсайдс С. Дискретная математика для программистов. Бином, Лаборатория знаний, 2010. – 632 с.
- Хантор Р. Проектирование и конструирование компиляторов. М.: Финансы и статистика. 1984. 232с.
- Харари Ф. Теория графов. М.: Мир, 1873. - 300 с.
- Харари Ф., Палмер Э. Перечисление графов. М.; МИР, 1977. - 324с.
- Яблонский С.В. Введение в дискретную математику. Высшая школа, 2012. – 384 с.
- Яблонский С.В., Гаврилов Г.П., Набебин А.А. Предполные классы в многозначных логиках. М.: Изд-во МЭИ, 1997. 144 с.
- IEEE Std. 754-2008. Standard for Floating-Point Arithmetic. – 58 р.
- Menezes A., van Oorshot P., Vanstone S. Handbook of applied cryptography. CRC Press. 1996. 780 p. Internet address: www.cacr.math.uwaterloo.ca/ha

- **Rosen K.H.** Discrete Mathematics and Its Applications. – 7th edition. McGraw-Hill, 2012. – 1071 p.

10.4 Программные средства

Для успешного освоения дисциплины, студент использует следующие программные средства:

- Программа WinLogica для построения и анализа комбинационных схем, содержащаяся в архиве [WinLogica.rar](#) – в подразделе «Домашнее задание 1» раздела «Материал» по дисциплине «Дискретная математика» системы LMS.
- Эмулятор Машины Тьюринга, установочный файл которого содержится в архиве [emt_setup.rar](#) в подразделе «Домашнее задание 2» раздела «Материал» по дисциплине «Дискретная математика» системы LMS.
- Эмулятор Машины Поста, установочный файл которого содержится в архиве [post_setup.rar](#) в подразделе «Домашнее задание 2» раздела «Материал» по дисциплине «Дискретная математика» системы LMS.
- Эмулятор алгоритмов Маркова, установочный файл которого содержится в архиве [markov_setup.rar](#) в подразделе «Домашнее задание 2» раздела «Материал» по дисциплине «Дискретная математика» системы LMS.
- Эмулятор рекурсивных функций, установочный файл которого содержится в архиве [rf_setup.rar](#) в подразделе «Домашнее задание 2» раздела «Материал» по дисциплине «Дискретная математика» системы LMS.

11 Материально-техническое обеспечение дисциплины

Для выполнения и защиты домашних заданий, а также проведения тестирования используется сетевой класс IBM совместимых компьютеров.

Авторы программы: _____ Авдошин С.М.
_____ Дворянский Л.В.
_____ Набебин А.А.