Приложение к ОПОП
«Организация и программирование интеллектуальных систем»

СПбГЭТУ «ЛЭТИ»
ПЕРВЫЙ ЭЛЕКТРОТЕХНИЧЕСКИЙ

МИНОБРНАУКИ РОССИИ

федеральное государственное автономное образовательное учреждение высшего образования
**«Санкт-Петербургский государственный электротехнический университет
«ЛЭТИ» им. В.И.Ульянова (Ленина)»
(СПбГЭТУ «ЛЭТИ»)**

РАБОЧАЯ ПРОГРАММА

дисциплины

«ДИСКРЕТНАЯ МАТЕМАТИКА И ТЕОРЕТИЧЕСКАЯ ИНФОРМАТИКА»

для подготовки бакалавров

по направлению

09.03.01 «Информатика и вычислительная техника»

по профилю

«Организация и программирование интеллектуальных систем»

Санкт-Петербург

2024

ЛИСТ СОГЛАСОВАНИЯ

Разработчики:

доцент, к.ф.-м.н. Рыбин С.В.

д.пед.н., доцент Поздняков С.Н.

Рабочая программа рассмотрена и одобрена на заседании кафедры АМ 15.01.2024, протокол № 6

Рабочая программа рассмотрена и одобрена учебно-методической комиссией ФКТИ, 24.01.2024, протокол № 1

Согласовано в ИС ИОТ

Начальник ОМОЛА Загороднюк О.В.

1 СТРУКТУРА ДИСЦИПЛИНЫ

Обеспечивающий факультет	ФКТИ
Обеспечивающая кафедра	АМ
Общая трудоемкость (ЗЕТ)	4
Курс	2
Семестр	3
Виды занятий	
Лекции (академ. часов)	34
Практические занятия (академ. часов)	34
Иная контактная работа (академ. часов)	1
Все контактные часы (академ. часов)	69
Самостоятельная работа, включая часы на контроль (академ. часов)	75
Всего (академ. часов)	144
Вид промежуточной аттестации	
Экзамен (курс)	2

2 АННОТАЦИЯ ДИСЦИПЛИНЫ

«ДИСКРЕТНАЯ МАТЕМАТИКА И ТЕОРЕТИЧЕСКАЯ ИНФОРМАТИКА»

Разделы современной математики, имеющие приложения в сфере информационных и компьютерных технологий, являются необходимыми при подготовке специалистов инженерных специальностей. Первый из них посвящен тем аспектам теории чисел, которые лежат в основе криптографических алгоритмов и механизмов шифрования. Во втором наряду с классическими вопросами теории многочленов рассматриваются алгоритмы, важные для компьютерной математики. Третий раздел объединяет классические комбинаторные идеи и их обобщения с прикладной проблематикой, в том числе, генерированием комбинаторных объектов, кодированием. Обсуждается техника работы с производящими функциями. Последний раздел посвящен дискретной теории вероятностей.

SUBJECT SUMMARY

«DISCRETE MATH»

Sections of modern mathematics, with applications in the field of information technology and computer technology, are necessary in the education of specialists of engineering specialties. The first of the sections devoted to those aspects of the theory of numbers, which are the basis of cryptographic algorithms and mechanisms like encryption. In the second section, along with the classic questions of the theory of polynomial algorithms are considered important for the computer mathematics, for example, the expansion of the polynomial on the square-free factors. The third category includes classic combinatorial ideas and their generalizations with application issues, including the generation of combinatorial objects, coding. We discuss the technique of working with generating functions. The last section is devoted to discrete probability theory.

3 ОБЩИЕ ПОЛОЖЕНИЯ

3.1 Цели и задачи дисциплины

1. Формирование достаточно высокой математической культуры является основной целью дисциплины. Для этого необходимо, познакомить студентов с основными понятиями, методами и алгоритмам работы с дискретными объектами, развить логическое мышление, привить навыки использования математических методов и основ математического моделирования в практической деятельности.

Методы и алгоритмы работы с дискретными объектами, являясь предметом изучения дисциплины, участвуют в развитии логического мышления и формировании навыков использования математических методов и основ математического моделирования в практической деятельности.

2. В рамках реализации цели решаются учебные задачи дисциплины:

-развить логическую культуру мышления студента;

-развить способность обосновывать свои суждения и выбор метода решения возникающих задач;

-сформировать навыки построения моделей и проведения расчетов для дискретных структур;

-научить студентов применять основные математические методы, используемые при моделировании реальных систем;

-выработать у студентов методологию математического подхода к анализу естественно-научных задач и проблем из других областей;

-выработать у студентов способность создать математическую модель рассматриваемого объекта и провести ее детальное исследование с анализом результатов.

3. В результате изучения дисциплины студенты должны приобрести знания по

следующей тематике:

1).Простые числа и методы факторизации.

2).Различные позиционные системы счисления (р-ичную, факториальную, смешанную).

3).Алгоритмы работы с длинными числами в р-ичной системе счисления.

4).Алгоритм быстрого возведения в степень в кольце вычетов .

5).Алгоритм Евклида в различных формах и вариациях.

6).Конечные и бесконечные цепные дроби. Разложение иррациональности в цепную дробь

7).Китайскую теорему об остатках, свойства функции Эйлера, теорему Эйлера.

8).Понятие примитивного многочлены и теоремы о приводимости и неприводимости многочленов над полем рациональных чисел, полем вычетов.

9).Алгоритм разложения на свободные от квадратов множители.

10).Основные комбинаторные конструкции и приемы.

11).Понятие производящей функции. Однородные и неоднородные рекуррентные уравнения.

4. В результате изучения дисциплины студенты должны приобрести следующие умения:

1).Выполнять действия в различных системах счисления и переходить от одного представления к другому.

2).Преобразовывать алгоритмы действий с длинными числами в р-ичной системе счисления в алгоритмы действий в других позиционных системах счисления.

3).Использовать алгоритм Евклида для нахождения НОД, сокращения дробей, решения диофантовых уравнений, нахождения обратного для классов вычетов, (разлагать в не-прерывную дробь).

4).Восстанавливать число по приведенной системе остатков.

5).Вычислять значения функции Эйлера.

6).Использовать теорему Эйлера для возведения в степень на классах вычетов.

5. В результате изучения дисциплины студенты должны приобрести навыки работы с алгоритмами работы с целыми числами, классами вычетов, многочленами, кодирования (RSA, Хаффмена, полиномиальным).

3.2 Место дисциплины в структуре ОПОП

Дисциплина изучается на основе ранее освоенных дисциплин учебного плана:

1. «Алгебра и геометрия»

2. «Информатика»

и обеспечивает изучение последующих дисциплин:

1. «Комбинаторика и теория графов»

2. «Учебная практика (технологическая (проектно-технологическая) практика)»

3. «Анализ данных в программах с открытым кодом»

4. «Математическая логика и теория алгоритмов»

5. «Введение в искусственный интеллект»

6. «Компьютерная графика»

7. «Производственная практика (технологическая (проектно-технологическая) практика)»

8. «Основы компьютерного зрения»

9. «Производственная практика (научно-исследовательская работа)»

3.3 Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

В результате освоения образовательной программы обучающийся должен достичь следующие результаты обучения по дисциплине:

Код компетенции/ индикатора компетенции	**Наименование компетенции/индикатора компетенции**
УК-1	Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач
УК-1.1	*Выполняет поиск необходимой информации, её критический анализ и обобщает результаты анализа для решения поставленной задачи*
ОПК-1	Способен применять естественнонаучные и общеинженерные знания, методы математического анализа и моделирования, теоретического и экспериментального исследования в профессиональной деятельности;
ОПК-1.1	*Знает основы высшей математики, физики, основы вычислительной техники и программирования*

4 СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1 Содержание разделов дисциплины

4.1.1 Наименование тем и часы на все виды нагрузки

№ п/п	Наименование темы дисциплины	Лек, ач	Пр, ач	ИКР, ач	СР, ач
1	Введение.	1			0
2	Целочисленные алгоритмы.	6	8		12
3	Модульная арифметика.	6	6		12
4	Система шифрования RSA.	4	2		10
5	Комбинаторика и производящие функции.	9	8		16
6	Арифметика многочленов.	4	6		15
7	Элементы дискретной теории вероятностей.	4	4	1	10
	Итого, ач	34	34	1	75
	Из них ач на контроль	0	0	0	35
	Общая трудоемкость освоения, ач/зе	144/4			

4.1.2 Содержание

№ п/п	Наименование темы дисциплины	Содержание
1	Введение.	История формирования дисциплины. Значение дисциплины в моделировании.
2	Целочисленные алгоритмы.	НОД, простые числа. Решето Эратосфена. Алгоритмы факторизации (метод пробных делителей и метод Ферма). Алгоритм Евклида, бинарный алгоритм. Обобщенный алгоритм Евклида. Анализ алгоритма Евклида, числа Фибоначчи. Диофантовы уравнения. Разложение числа в цепную дробь. Свойства и вычисление подходящих дробей. Бесконечные цепные дроби. Наилучшие приближения.
3	Модульная арифметика.	Арифметика и свойства сравнений. Линейные сравнения. Китайская теорема об остатках. Система остаточных классов (RNS). Функция Эйлера и ее свойства. Теорема Эйлера-Ферма. Быстрое возведение числа в степень в кольце.
4	Система шифрования RSA.	Применение теоремы Эйлера в криптографии. Система шифрования RSA. Электронная подпись. Электронные деньги. Простейшие атаки на систему RSA.

№ п/п	Наименование темы дисциплины	Содержание
5	Комбинаторика и производящие функции.	Алгоритм Хаффмана. Лексикографический и антилексикографический порядок. Генерация k -элементных подмножеств. Перечислительная комбинаторика. Код Грея. Перечисление перестановок. Разбиения чисел. Принцип включения-исключения. Задача о беспорядках. Производящие функции. Решение однородного линейного рекуррентного уравнения. Частные решения. Решение неоднородного линейного рекуррентного уравнения.
6	Арифметика многочленов.	Арифметика многочленов. Алгоритм Евклида и китайская теорема для многочленов. Интерполяционная формула Лагранжа. Полиномиальное кодирование.
7	Элементы дискретной теории вероятностей.	Основные определения, условные вероятности и формула Байеса. Случайные величины. Математическое ожидание и дисперсия. Схема Бернулли.

4.2 Перечень лабораторных работ

Лабораторные работы не предусмотрены.

4.3 Перечень практических занятий

Наименование практических занятий	Количество ауд. часов
1. Алгоритм Евклида, бинарный алгоритм.	2
2. Линейное представление НОД. Диофантовы уравнения.	2
3. Разложение иррациональности в цепную дробь.	4
4. Китайская теорема об остатках.	2
5. Линейные сравнения.	4
6. Алгоритм RSA кодирования.	2
7. Алгоритм Хаффмана.	2
8. Принцип включения-исключения.	2
9. Кодирование перестановок.	2
10. Алгоритм Евклида для многочленов. Линейное представление НОД в различных полях.	2
11. Интерполяционный многочлен Лагранжа.	2
12. Полиномиальное кодирование.	2
13. Однородные и неоднородные линейные рекуррентные уравнения с постоянными коэффициентами.	2
14. Дискретные случайные величины.	4
Итого	34

4.4 Курсовое проектирование

Курсовая работа (проект) не предусмотрены.

4.5 Реферат

Реферат не предусмотрен.

4.6 Индивидуальное домашнее задание

В процессе обучения по дисциплине «**Дискретная математика и теоретическая информатика**» студент обязан выполнить Индивидуальное домашнее задание (ИДЗ). Задачи ИДЗ охватывают весь спектр тематики, рассматриваемой в семестре, и содержит задачи на:

- применение целочисленных алгоритмов,
- применение модульной арифметики;
- применение полиномиальных алгоритмов,
- построение элементарных систем шифрования,
- использование комбинаторики и производящих функций.

Требования по оформлению ИДЗ:

- Формат оформления: произвольный формат (печатный или рукописный). При выборе печатного формата следует использовать редакторы Word или Excel. При выборе рукописного формата следует оформить работу на двойных листах в клетку или листах формата А4, или в тетради (в клетку) объемом не более 12 листов.
- При рукописном оформлении ИДЗ следует писать аккуратно черными или синими чернилами, с обязательным использованием линейки и карандаша при выполнении чертежей. При печатном оформлении ИДЗ рекомендуется использовать шрифт Times New Roman, Calibri или Ariel; размер шрифта 12-14 пунктов, межстрочный интервал 1,15-1,5 пунктов.

Каждую задачу следует оформлять на новом листе.

- Таблицы и рисунки следует оформлять, придерживаясь сквозного просмотра. Т.е. если в задаче предусмотрена таблица или рисунок, то они должны быть приведены внутри или в конце решаемой задачи. Общее приложение для все рисунков и таблиц не предусматривается.
- Объем ИДЗ зависит только от количества задач и/или заданий. каждая задача должна содержать исходные данные, решение и ответ.
- Количество используемых источников не ограничено.
- Каждое ИДЗ состоит из: титульного листа (название дисциплины, ФИО, звание преподавателя, номер группы, ФИО студента, номер варианта, дата сдачи работы) списка решенных задач и/или заданий, списка используемых источников.
- Формат сдачи работы зависит от общих требований Университета (при очном обучении - ИДЗ сдается преподавателю в письменном виде или печатном виде; при дистанционном обучении - в печатном или электронном виде работы размещается в Moodle или отправляются преподавателю на электронную почту).

Примерный вариант ИДЗ по дисциплине "Дискретная математика и теоретическая информатика"

1. Решить диофантово уравнение $5658x + 6325y = 161$

2. Найти наименьшее натуральное число x, удовлетворяющее условиям $x \equiv 6 \bmod 36$; $x \equiv 5 \bmod 11$; $x \equiv 6 \bmod 19$; $x \equiv 17 \bmod 23$;

3. Найти остаток от деления 231119 на 44.

4. По формуле Лагранжа найти многочлен p не выше 4-ой степени, удовлетворяющий условиям: $p(-2) = 18$; $p(-3) = 32$; $p(2) = -38$; $p(-4) = 10$; $p(-1) = 4$; 5. Найти рациональные корни: $x4 - 5x3 - 6x2 + 7x - 2$

6. Вычислить 7/37 в кольце вычетов по модулю 55.

7. Найти представление рационального числа 324/247 непрерывной дробью.

8. Найти остаток от деления многочлена $x^5 + 2x^3 + x^2 + 2x + 1$ на $x^3 + x^2 + x + 1$ в кольце $Z/3Z[x]$.

9. Среди 25 целых чисел, 6 кратно 11, 16 кратно 3, 2 кратно 121, 2 кратно 33, 1 кратно 363. Определить, сколько среди них кратно 11 или 3, но не кратно 121.

10. Все перестановки 7 чисел (1;2;3;4;5;6;7) упорядочены в лексикографическом порядке. Какой по счету идет перестановка 5274631?

11. С помощью алгоритма Хаффмана построить код Шеннона-Фэно для текстового сообщения, состоящего из символов “щ”, “ъ”, “ы”, “ю”, “ь”, “э” с частотами соответственно 43, 42, 81, 11, 94, 17.

14. а) Представьте $\sqrt{142}$ в виде периодической цепной дроби; б) вычислите ее с точностью до $\varepsilon = 10^{-4}$.

15. Русское слово из четырех букв закодировано при помощи алгоритма RSA открытым ключом ($e = 7$, $m = 33$). Шифрованное сообщение имеет вид (12; 25; 13; 29). Подберите закрытую часть ключа и прочитайте исходное слово. Буквам русского алфавита соответсвуют числа в диапазоне от 2 до 32 (исключены буквы “е” и “ъ”).

4.7 Доклад

Доклад не предусмотрен.

4.8 Кейс

Кейс не предусмотрен.

4.9 Организация и учебно-методическое обеспечение самостоятельной работы

Изучение дисциплины сопровождается самостоятельной работой студентов с рекомендованными преподавателем литературными источниками и информационными ресурсами сети Интернет.

Планирование времени для изучения дисциплины осуществляется на весь период обучения, предусматривая при этом регулярное повторение пройденного материала. Обучающимся, в рамках внеаудиторной самостоятельной работы, необходимо регулярно дополнять сведениями из литературных источников материал, законспектированный на лекциях. При этом на основе изучения рекомендованной литературы целесообразно составить конспект основных положений, терминов и определений, необходимых для освоения разделов учебной дисциплины.

Особое место уделяется консультированию, как одной из форм обучения и контроля самостоятельной работы. Консультирование предполагает особым образом организованное взаимодействие между преподавателем и студентами, при этом предполагается, что консультант либо знает готовое решение, которое он может предписать консультируемому, либо он владеет способами деятельности, которые указывают путь решения проблемы.

Текущая СРС	**Примерная трудоемкость, ач**
Работа с лекционным материалом, с учебной литературой	10
Опережающая самостоятельная работа (изучение нового материала до его изложения на занятиях)	8
Самостоятельное изучение разделов дисциплины	0
Выполнение домашних заданий, домашних контрольных работ	6
Подготовка к лабораторным работам, к практическим и семинарским занятиям	12
Подготовка к контрольным работам, коллоквиумам	4
Выполнение расчетно-графических работ	0
Выполнение курсового проекта или курсовой работы	0

Текущая СРС	Примерная трудоемкость, ач
Поиск, изучение и презентация информации по заданной проблеме, анализ научных публикаций по заданной теме	0
Работа над междисциплинарным проектом	0
Анализ данных по заданной теме, выполнение расчетов, составление схем и моделей, на основе собранных данных	0
Подготовка к зачету, дифференцированному зачету, экзамену	35
ИТОГО СРС	75

5 Учебно-методическое обеспечение дисциплины

5.1 Перечень основной и дополнительной литературы, необходимой для освоения дисциплины

№ п/п	Название, библиографическое описание	К-во экз. в библ.
Основная литература		
1	Новиков, Федор Александрович. Дискретная математика для программистов [Текст] : для студентов вузов по направлению подгот. ”Информатика и вычисл. техника” / Ф.А. Новиков, 2008. -383 с.	38
2	Поздняков, Сергей Николаевич. Дискретная математика [Текст] : учеб. для вузов по направлениям подгот. ”Информатика и вычисл. техника”, ”Информационные системы”, ”Информационная безопасность” / С.Н. Поздняков, С.В. Рыбин, 2008. -448 с.	492
3	Поздняков, Сергей Николаевич. Компьютерная математика [Текст] : учеб. пособие / С.Н. Поздняков, С.В. Рыбин, 2005. -64 с.	5
4	Новиков Ф.А. Дискретная математика: Учебник для вузов. 3-е изд. Стандарт третьего поколения [Электронный ресурс] / Ф.А. Новиков, 2017. -496 с.	неогр.
Дополнительная литература		
1	Новиков Ф.А. Дискретная математика для программистов [Текст] : Учеб. / Ф.А.Новиков, 2000. -301 с.	115
2	Кузнецов, Олег Петрович. Дискретная математика для инженера [Текст] : монография / О.П.Кузнецов, Г.М.Адельсон-Вельский, 1988. -480 с.	70
3	Кузнецов, Олег Петрович. Дискретная математика для инженера [Текст] / О. П. Кузнецов, 2007. -394, [1] с.	неогр.

5.2 Перечень ресурсов информационно-телекоммуникационной сети «Интернет», используемых при освоении дисциплины

№ п/п	Электронный адрес
1	Обсуждение и C++ реализация алгоритмов дискретной математики.http://www.arvi fox.com/wp-content/uploads/2017/10/e-maxx_algo.pdf
2	С. Н. Поздняков С. В. Рыбин Дискретная математика.https://students.iposov.spb.ru /21spring/dm/Rybin-Pozdnkov-20-06-2021.pdf

5.3 Адрес сайта курса

Адрес сайта курса: https://vec.etu.ru/moodle/course/view.php?id=21167

6 Критерии оценивания и оценочные материалы

6.1 Критерии оценивания

Для дисциплины «Дискретная математика и теоретическая информатика» предусмотрены следующие формы промежуточной аттестации: экзамен.

Экзамен

Оценка	Описание
Неудовлетворительно	Курс не освоен. Студент испытывает серьезные трудности при ответе на ключевые вопросы дисциплины
Удовлетворительно	Студент в целом овладел курсом, но некоторые разделы освоены на уровне определений и формулировок теорем
Хорошо	Студент овладел курсом, но в отдельных вопросах испытывает затруднения. Умеет решать задачи
Отлично	Студент демонстрирует полное овладение курсом, способен применять полученные знания при решении конкретных задач.

Особенности допуска

Форма проведения, регламент экзамена и правила выставления оценки определяются лектором для каждого потока, и сдаются на кафедру вместе с экзаменационными вопросами до начала экзаменационной сессии.

Текущая аттестация студентов может учитываться при проведении экзамена в одном из двух видов:

-«допуск» до экзамена. Допущенными до экзамена считаются студенты, получившие по итогам текущей аттестации оценку выше порогового уровня (имеющие в сводных электронных ведомостях кафедры итоговую оценку 3, 4, 5).

-«часть экзамена». Доля участия суммарной многобалльной оценки текущей аттестации (оценки за практические занятия) в экзаменационной оценке определяется лектором и доводится до сведения студентов и ассистентов в начале семестра.

Особенностью проведения промежуточной аттестации по дисциплине ”Дискретная математика и теоретическая информатика” является включение в экзаменационный билет задач по основным разделам дисциплины. Студенту предлагается решить эти экзаменационные задачи, а при устном ответе указать с какими теоретическими положениями курса связаны алгоритмы их решения.

6.2 Оценочные материалы для проведения текущего контроля и промежуточной аттестации обучающихся по дисциплине

Вопросы к экзамену

№ п/п	Описание
1	НОД, простые числа.
2	Решето Эратосфена.
3	Алгоритмы факторизации (метод пробных делителей и метод Ферма).
4	Алгоритм Евклида, бинарный алгоритм.
5	Обобщенный алгоритм Евклида.
6	Анализ алгоритма Евклида, числа Фибоначчи.
7	Диофантовы уравнения.
8	Разложение числа в цепную дробь.

9	Свойства и вычисление подходящих дробей.
10	Бесконечные цепные дроби.
11	Наилучшие приближения.
12	Арифметика и свойства сравнений.
13	Линейные сравнения.
14	Китайская теорема об остатках.
15	Система остаточных классов (RNS).
16	Функция Эйлера и ее свойства.
17	Теорема Эйлера-Ферма.
18	Быстрое возведение числа в степень в кольце.
19	Применение теоремы Эйлера в криптографии.
20	Система шифрования RSA.
21	Электронная подпись.
22	Электронные деньги.
23	Простейшие атаки на систему RSA.
24	Алгоритм Хаффмана.
25	Лексикографический и антилексикографический порядок.
26	Генерация k -элементных подмножеств.
27	Перечислительная комбинаторика.
28	Код Грея.
29	Перечисление перестановок.
30	Разбиения чисел.
31	Принцип включения-исключения.
32	Задача о беспорядках.
33	Производящие функции.
34	Решение однородного линейного рекуррентного уравнения.
35	Частные решения линейного рекуррентного уравнения
36	Решение неоднородного линейного рекуррентного уравнения.
37	Арифметика многочленов.
38	Алгоритм Евклида и китайская теорема для многочленов.
39	Интерполяционная формула Лагранжа.
40	Полиномиальное кодирование.
41	Основные определения, условные вероятности и формула Байеса.
42	Случайные величины. Математическое ожидание и дисперсия.
43	Схема Бернулли.

Форма билета

Министерство науки и высшего образования Российской Федерации

ФГАОУ ВО «Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» имени В.И. Ульянова (Ленина)»

_____

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № _

Дисциплина **Дискретная математика и теоретическая информатика** ФКТИ

Задача 1.

1.1. После некоторого элементарного шага бинарного алгоритма Евклида нахождения НОД были получены два числа 1011001 и 100110001. Какими могли быть числа непосредственно перед выполнением этого шага?

1.2. N=14 M=49*1024^k+14. Сколько ‘элементарных шагов сделает бинарный алгоритм Евклида для чисел N и M в зависимости от k?. (другая версия N=3*4^n M=5*8^m)

1.3. N=1 M=3*2^k+5*2^n Сколько шагов сделает алгоритм для этих чисел?

Задача 2.

2.1. Привести пример многочлена P(x), который не имеет многочленов-делителей первой степени ни над Q, ни над Z2, ни над Z3. Ответ обосновать.

2.2. Привести пример многочлена P(x), который дает разное число неприводимых множителей при разложении над Q, Z2 и Z3. Ответ обосновать.

2.3. Привести пример двух многочленов P(x) и Q(x), таких что разложение многочлена M(x)=P(x)Q(x) на свободные от квадратов множители даст другой состав множителей чем разложение P(x) и Q(x) независимо. Ответ обосновать.

Задача 3.

3.1. На отрезке от 999 до 1999 найдите два разные числа с одинаковым значением функции Эйлера.

3.2. Найдите количество чисел, взаимно простых с 2000 на отрезке от 999 до 1999.

3.3. Найдите количество неотрицательных решений уравнения НОД(x; 21^20)=1, не превышающих 1999.

УТВЕРЖДАЮ

Заведующий кафедрой С.Н. Поздняков

Образцы задач (заданий) для контрольных (проверочных) работ

Примерные вопросы и варианты практических заданий заданий для коллоквиумов по темам ”Основные понятия комбинаторики ” и ”Арифметика многочленов”

Вопросы по теме ”Основным понятиям комбинаторики”

1. Правила суммы и произведения, типы выборок (дать определение, пояснить на примере).
2. Доказать, что $\overline{A}_n^r = n^r$.
3. Доказать, что $A_n^r = n(n-1)(n-2)...(n-(r-1)) = \dfrac{n!}{(n-r)!}$ при $n \geq r$, и $A_n^r = 0$ при $n < r$.
4. Доказать, что $C_n^r = \dfrac{n!}{(n-r)!r!}$ при $n \geq r$, и $C_n^r = 0$ при $n < r$.
5. Доказать, что $\overline{C}_n^r = C_{r+n-1}^r$.
6. Доказать теорему о числе упорядоченных разбиений множества на k подмножеств.
7. Доказать теорему о числе слов, записанных с помощью определённого набора букв.
8. Доказать теорему о числе неупорядоченных разбиений множества на k подмножеств.
9. Полиномиальная формула.
10. Формула включений и исключений.
11. Следствие из формулы включений и исключений и её особая форма записи.
12. Задача о беспорядках.

Вопросы по теме "Арифметика многочленов"

1. Определение кольца. Простейшие следствия из аксиом. Примеры. Целостность.
2. Евклидовы кольца. Евклидовость **Z**. Неприводимые и простые элементы. Идеалы, главные идеалы. Евклидово кольцо как кольцо главных идеалов.
3. Основная теорема арифметики.
4. Кольцо вычетов **Z**/n**Z**. Китайская теорема об остатках.
5. Определение поля. **Z**/p**Z** как поле. Поле частных целостного кольца.
6. Определение гомоморфизма и изоморфизма колец. Фактор-кольцо.
7. Теорема о гомоморфизме.
8. Кольцо многочленов от одной переменной. Целостность и евклидовость кольца многочленов от одной переменной над полем. Поле рациональных функций.
9. Лемма Гаусса. Факториальные кольца. Факториальность кольца многочленов от нескольких переменных над полем.
10. Присоединение переменной к полю. Поле разложение многочлена. Кратные корни. Теорема Виета.
11. Интерполяция Лагранжа и Эрмита. Формальное и функциональное равенство многочленов.
12. Алгебраическое замыкание и его существование.
13. Комплексные числа. Решение квадратных уравнений в **C**.
14. Основная теорема алгебры (формулировка и набросок доказательства).
15. Разложение рациональной функции в простейшие дроби над **C** и над **R**.

Практические задания по теме ”**Арифметика многочленов**”

1. Пользуясь схемой Горнера, выполните деление с остатком:

1) $2x^5+7x^4-8x^2+3x-5$ на $x+2$,

2) $3x^6-2x^4+6x^3-8x+11$ на $x+1{,}5$,

3) $x^4-8x^3+24x^2-50x+90$ на $x-2$,

4) $x^4+2ix^3-(1+i)x^2-3x+7$ на $x+i$,

5) $x^4-2ix^3-(1-i)x^2-3x+7$ на $x-i$,

6) $4x^5+(2-i)x^4-5ix^3+(i-1)x-2i$ на $x+1-i$.

2. Пользуясь схемой Горнера, разложить многочлен f (x) по степеням x - x0 :

1) $f(x)=x^4+2x^3-3x^2-2x+3,\ x_0=-1,$

2) $f(x)=x^4-7x^3+12x^2-24x+24,\ x_0=2,$

3) $f(x)=(x-1)^4+2(x-1)^3-3(x-1)^2-7,\ x_0=2,$

4) $f(x)=(x-3)^5+5(x-3)^4-3(x-3)^3+2(x-3)^2+2(x-3)+3,\ x_0=2,$

5) $f(x)=(x+3)^4-5(x+3)^3+7(x+3)+1,\ x_0=0,$

6) $f(x)=x^4+2ix^3-(1+i)x^2-x+3i,\ x_0=-i,$

7) $f(x)=x^4-2ix^3-(1-i)x^2-x-3i,\ x_0=i.$

3. Пользуясь схемой Горнера, найти кратность корня x0 многочлена f (x) :

1) $f(x)=x^5+6x^4+11x^3+2x^2-12x-8,\ x_0=-2,$

2) $f(x)=5x^4+14x^3+12x^2+2x-1,\ x_0=-1,$

3) $f(x)=x^5+7x^4+16x^3+8x^2-16x-16,\ x_0=-2,$

4) $f(x)=x^6-6x^4-4x^3+9x^2+12x+4,\ x_0=-1,$

5) $f(x)=x^5-5x^4+40x^2-80x+48,\ x_0=2$

6) $f(x)=x^5-5x^4+7x^3-2x^2+4x-8,\ x_0=2.$

4. Пользуясь алгоритмом Евклида, для данных многочленов f (x) и g(x) подобрать многочлены u(x) и v(x) так, чтобы u(x)· f (x) +v(x)· g(x)= d(x), где d(x) – наибольший общий делитель многочленов f (x) и g(x):

1) $f(x)=x^4+2x^3-x^2-4x-2,$

$g(x)=x^4+x^3-x^2-2x-2.$

2) $f(x)=x^5+3x^4+x^3+x^2+3x+1,$

$g(x)=x^4+2x^3+x+2.$

3) $f(x)=x^4+6x^3+11x^2+4x-4,$

$g(x)=x^4+5x^3+8x^2+3x-3.$

4) $f(x)=x^7-3x^5-x^4+2x^3+2x^2-3x+1,$

$g(x)=x^4-3x^2+1.$

5) $f(x)=3x^3+2x^2+x+2,$

$g(x)=x^2-x+1.$

6) $f(x)=x^4-x^3-4x^2+4x+1,$

$g(x)=x^2-x-1.$

7) $f(x)=3x^3+7x^2+6x+4,$

$g(x)=x^2+x+1.$

8) $f(x)=x^4+3x^3-x^2-3x+1,$

$g(x)=x^2+x-1.$

9) $f(x)=x^5-5x^4-2x^3+12x^2-2x+12,$

$g(x)=x^3-5x^2-3x+17.$

10) $f(x)=x^5-12x^3-14x^2+x+16,$

$g(x)=x^3-2x^2-10x+10.$

Весь комплект контрольно-измерительных материалов для проверки сформированности компетенции (индикатора компетенции) размещен в закрытой части по адресу, указанному в п. 5.3

6.3 График текущего контроля успеваемости

Неделя	Темы занятий	Вид контроля
2	Целочисленные алгоритмы. Модульная арифметика. Комбинаторика и производящие функции. Система шифрования RSA. Арифметика многочленов.	
3		
4		
5		
6		
7		
8		
9		
10		
11		
12		
13		
14		
15		ИДЗ / ИДРГЗ / ИДРЗ
16	Арифметика многочленов. Комбинаторика и производящие функции.	
17		Коллоквиум

6.4 Методика текущего контроля

на лекционных занятиях

Текущий контроль включает в себя контроль посещаемости (не менее ***80*** % занятий). В течение семестра проводится коллоквиум по основным теоретическим положениям курса. Каждый студент получает вопрос по теоретической части, после чего ему предоставляется время для подготовки ответа. При обсуждении ответа преподаватель может задать несколько уточняющих вопросов по использованию этих теоретических положений при решении задач. В случае если студент демонстрирует достаточное знание вопроса, коллоквиум по теоретической части считается сданным.

на практических занятиях

В процессе обучения по дисциплине «**Дискретная математика и теоретическая информатика**» студент обязан выполнить Индивидуальное домашнее задание (ИДЗ) содержательно охватывает весь спектр рассматриваемой те-

матики, поэтому предусмотрено выполнение ИДЗ с 2-й по 14-ю неделю обучения по мере продвижения по темам. После его выполнения предусматривается проверка ИДЗ преподавателем на 15 неделе, а далее проведение коллоквиума на 16-17 неделях, на котором осуществляется защита ИДЗ и выполненной работы над ошибками, если это необходимо. Выполнение ИДЗ и оформление решения студентами осуществляется индивидуально.

Текущий контроль включает в себя выполнение, сдачу в срок ИДЗ и его защиту. Примерный вариант ИДЗ приведен в оценочных материалах для проведения ТК и промежуточной аттестации.

В ходе проведения семинарских и практических занятий целесообразно привлечение студентов к как можно более активному участию в дискуссиях, решении задач, обсуждениях и т. д. При этом активность студентов также может учитываться преподавателем, как один из способов текущего контроля на практических занятиях.

самостоятельной работы студентов

Контроль самостоятельной работы студентов осуществляется на лекционных, практических занятиях студентов по методикам, описанным выше.

Коллоквиум проводится на основе вопросов к экзамену, изученных до момента проведения коллоквиума.

Критерии оценивания:

”отлично” - ответ дан без ошибок, обоснован теоретически и проиллюстрирован примерами;

”хорошо”- ответ дан без ошибок, проиллюстрирован примерами, но обоснования не всегда полны;

”удовлетворительно” - ответ дан без ошибок, проиллюстрирован примерами, но не все обоснования приведены корректно;

”неудовлетворительно”- в ответе есть ошибки, либо студент не видит связи между приводимыми формулами и утверждениями, не понимает их смысла.

Контроль самостоятельной работы студентов осуществляется на лекционных, практических занятиях студентов по методикам, описанным выше.

Методика оценивания контрольных работ и ИДЗ:

”**неудовлетворительно**” (или 2), если верно решено меньше 60% заданий, но более 29%;

”**удовлетворительно**” (или 3), если верно решено меньше 75% заданий, но более 59%;

”**хорошо**” (или 4), если верно решено меньше 89% заданий, но более 74%;

”**отлично**” (или 5), если верно решено более 90% заданий.

7 Описание информационных технологий и материально-технической базы

Тип занятий	Тип помещения	Требования к помещению	Требования к программному обеспечению
Лекция	Лекционная аудитория	Количество посадочных мест – в соответствии с контингентом, рабочее место преподавателя: меловая или маркерная доска	
Практические занятия	Аудитория	Количество посадочных мест – в соответствии с контингентом, рабочее место преподавателя: меловая или маркерная доска	
Самостоятельная работа	Помещение для самостоятельной работа	Оснащено компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.	1) Windows XP и выше; 2) Microsoft Office 2007 и выше

8 Адаптация рабочей программы для лиц с ОВЗ

Адаптированная программа разрабатывается при наличии заявления со стороны обучающегося (родителей, законных представителей) и медицинских показаний (рекомендациями психолого-медико-педагогической комиссии). Для инвалидов адаптированная образовательная программа разрабатывается в соответствии с индивидуальной программой реабилитации.

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

№ п/п	Дата	Изменение	Дата и номер протокола заседания УМК	Автор	Начальник ОМОЛА