Федеральное государственное бюджетное образовательное учреждение
высшего образования
Московский государственный университет имени М.В. Ломоносова
Факультет вычислительной математики и кибернетики

УТВЕРЖДАЮ
декан факультета вычислительной
математики и кибернетики

_____/И.А. Соколов /
«___» _____2024г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Введение в теорию чисел и приложения

Уровень высшего образования:

магистратура

Направление подготовки / специальность:

01.04.02 "Прикладная математика и информатика" (3++)

Направленность (профиль) ОПОП:

Кибербезопасность

Форма обучения:

очная

Рабочая программа рассмотрена и утверждена
на заседании Ученого совета факультета ВМК
(протокол № ___ от _____)

Москва 2024

Рабочая программа дисциплины (модуля) разработана в соответствии с самостоятельно разрабатываемым образовательным стандартом МГУ имени М.В. Ломоносова для реализуемых основных профессиональных образовательных программ высшего образования по направлению подготовки 01.04.02 "Прикладная математика и информатика" (3++).

1. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОПОП ВО:

Настоящая дисциплина включена в учебный план по направлению 01.04.02 "Прикладная математика и информатика" (3++), профиль Кибербезопасность и входит в Базовую часть программы (Модуль "Программное обеспечение современных вычислительных систем").

Дисциплина является кафедральным (вариативным) курсом и изучается по выбору студента.

Дисциплина рассчитана на студентов, знакомых с основными понятиями и результатами линейной алгебры и комплексного анализа, а также владеющих основами языка программирования Python.

2. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ:

Курс является введением в современную теорию чисел с акцентом на приложения. Дается теоретический материал, необходимый для последующего изучения прикладных курсов по криптографии и теории кодирования, а также продвинутых курсов по теории чисел и алгебраической геометрии. Теоретический материал подкрепляется вычислительными задачами и примерами с использованием системы компьютерной алгебры SageMath. Курс не является введением в криптографию и теорию кодирования, хотя на семинарах и рассматриваются некоторые криптографические схемы и элементы теории кодов. Курс также не является введением в вычислительные алгоритмы теории чисел и алгебры. Помимо приложений в криптографии и теории кодирования, дается связь с задачами современного анализа данных, например, приложения к задачам оптимального дизайн экспериментов.

3. РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ):

Компетенции выпускников, частично формируемые при реализации дисциплины (модуля):

Планируемые результаты обучения по дисциплине (модулю)		
Содержание и код компетенции.	**Индикатор (показатель) достижения компетенции**	**Планируемые результаты обучения по дисциплине, сопряженные с индикаторами достижения компетенций**
ОПК-1. Способность формулировать и решать актуальные задачи в области фундаментальной и прикладной математики. **ОПК-4.** Способность комбинировать и адаптировать современные информационно-коммуникац	**СПК-ВТЧП-1М.1.** Владение основными понятиями и методами элементарной теории чисел **СПК-ВТЧП-1М.2.** Владение основными понятиями и результатами связанными с	**Знать** ● Основные понятия, определения и результаты элементарной теории чисел ● Основные понятия, определения и результаты теории конечных полей

ионные технологии для решения задач в области профессиональной деятельности с учетом требований информационной безопасности. **ПК-2.** Способность в рамках задачи, поставленной специалистом более высокой квалификации, проводить научные исследования и (или) осуществлять разработки в области прикладной математики и информатики с получением научного и (или) научно-практического результата; **СПК-ВТЧП-1М.** Способность формулировать и решать задачи в области теории чисел и ее приложений, используя современные информационно-коммуникационные технологии.	конечными полями и многочленами на ними **СПК-ВТЧП-1М.3.** Знакомство с основными понятиями и методами алгебраической теории чисел (числовые поля и p-адические числа) **СПК-ВТЧП-1М.4.** Знакомство с методами аналитической теории чисел (ряды Дирихле и оценки тригонометрических сумм) **СПК-ВТЧП-1М.5.** Владение системой компьютерной алгебры SageMath для решения задач теории чисел и алгебры **СПК-ВТЧП-1М.6.** Понимание приложений теории чисел для задач криптографии **СПК-ВТЧП-1М.7.** Понимание приложений теории чисел для задач теории кодирования	● Основные понятия, определения и результаты алгебраической теории чисел ● Основные направления приложений теории чисел в криптографии и теории кодирования **Уметь** ● Решать задачи теории чисел, используя элементарные, комбинаторные, аналитические и алгебраические методы ● Применять системы компьютерной алгебры и символьных вычислений для решения задач алгебры и теории чисел ● Применять методы теории чисел к формализации постановок прикладных задач, включая криптографию и теорию кодирования **Владеть** ● Навыками работы в системе компьютерной алгебры SageMath

4. ФОРМАТ ОБУЧЕНИЯ И ОБЪЁМ ДИСЦИПЛИНЫ (МОДУЛЯ)

Формат обучения: занятия проводятся с использованием меловой или маркерной доски, интерактивные материалы демонстрируются с помощью ноутбука и проектора.

Объем дисциплины (модуля) составляет 112 академических часов, в том числе 68 академических часов, отведенных на контактную работу обучающихся с преподавателем, 44 академических часа на самостоятельную работу обучающихся.

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ), СТРУКТУРИРОВАННОЕ ПО ТЕМАМ (РАЗДЕЛАМ) С УКАЗАНИЕМ ОТВЕДЕННОГО НА НИХ КОЛИЧЕСТВА АКАДЕМИЧЕСКИХ ЧАСОВ И ВИДЫ УЧЕБНЫХ ЗАНЯТИЙ

5.1. Структура дисциплины (модуля) по темам (разделам) с указанием отведенного на них количества академических часов и виды учебных занятий (в строгом соответствии с учебным планом)

Наименование разделов и тем дисциплины (модуля), **Форма промежуточной аттестации по дисциплине (модулю)**	**Номинальные трудозатраты обучающегося**			**Всего академических часов**	**Форма текущего контроля успеваемости* (наименование)**
	Контактная работа (работа во взаимодействии с преподавателем) Виды контактной работы, академические часы		**Самостоятельная работа обучающегося, академические часы**		
	Занятия лекционного типа	Занятия семинарского типа			
Раздел I. Элементарная теория чисел					
Тема 1. Простые числа	2	2	2	6	
Тема 2. Сравнения	2	2	2	6	
Тема 3. Первообразные корни	2	2	2	6	
Тема 4. Квадратичные вычеты	2	2	2	6	
Раздел II. Конечные поля					
Тема 5. Конечные поля. Соответствие Галуа	2	2	2	6	
Тема 6. Корни из единицы. Круговой многочлен.	2	2	2	6	
Тема 7. Норма и след. Характеры. Суммы Гаусса.	2	2	2	6	
Тема 8. Тригонометрические суммы. Уравнения над конечными полями	2	2	2	6	
Тема 9. Дзета функция Артина, соотношение Хассе-Дэвенпорта	2	2	2	6	коллоквиум

Раздел III. p-адические числа					
Тема 10. p-адические числа: элементарное определение и свойства	2	2	2	6	
Тема 11. Аксиоматическое определение поля p-адических чисел, метризованные поля	2	2	2	6	
Тема 12. Лемма Гензеля, сравнения и кольцо целых p-адических чисел	2	2	2	6	
Раздел IV. Числовые поля					
Тема 13. Кольцо целых гауссовых чисел, числовые поля	2	2	4	8	
Тема 14. Делимость в кольцах целых алгебраических чисел	2	2	4	8	
Тема 15. Квадратичное поле и круговое поле	2	2	4	8	
Раздел V. Теорема Дирихле					
Тема 16. Ряды Дирихле	2	2	4	8	
Тема 17. Распределение простых чисел арифметической прогрессии	2	2	4	8	
Промежуточная аттестация (зачет)					экзамен
Итого	**34**	**34**	**44**	**112**	

5.2. Содержание разделов (тем) дисциплины

Курс состоит из пяти разделов. Первый раздел является введением и посвящен элементарной теории чисел. Рассматриваются свойства делимости в кольце целых рациональных чисел, изучается кольцо классов вычетов, исследуются свойства основных арифметических функций, рассматриваются вопросы разрешимости некоторых сравнений и диофантовых уравнений.

Во втором разделе изучается один из основных объектов теоретико-числовых приложений – конечные поля. Работа с многочленами над конечными полями также является ключевым навыком для приложений в криптографии и теории кодирования. Вводится понятие характера конечной абелевой группы, доказываются некоторые факты о полных и неполных тригонометрических суммах. В последней лекции второго

раздела затрагиваются вопросы алгебраической геометрии над конечными полями: вводится понятие дзета-функции алгебраической поверхности над конечным полем, на примере одной гиперповерхности элементарными методами доказывается рациональность соответствующей дзета-функции.

Третий раздел посвящен введению в p-адические числа и метризованные поля. p-адический анализ является важным инструментом современной криптографии, а область p-адических динамических систем имеет много других приложений. В первой лекции раздела дается прямое построение кольца целых p-адических чисел, рассматриваются его основные арифметические свойства, изучаются вопросы сходимости p-адических последовательностей и рядов. Далее рассматривается общий случай метризованных полей и их пополнений. Доказывается теорема Островского о классификации всех пополнений поля рациональных чисел. Разбирается несколько случаев леммы Гензеля, которая может быть использована в качестве инструмента для решения алгебраических уравнений в p-адических числах и сравнений. Формулируется теорема Минковского-Хассе и локально-глобальный принцип (принцип Хассе).

В четвертом разделе рассматриваются некоторые вопросы числовых полей и колец. Порядки и кольца алгебраических чисел играют важную роль при изучении теории решеток, а также арифметики эллиптических кривых. Доказывается однозначность разложения на множители в кольце гауссовых чисел. Даются примеры колец целых алгебраических чисел, в которых разложение на простые множители не является однозначным. Вводится понятие евклидовых и дедекиндовых колец. Обзорно приводятся результаты приложения теории Галуа к вопросам делимости в порядках числовых полей. Исследуется связь с представимостью чисел суммами квадратов и разрешимостью некоторых диофантовых уравнений. Более подробно изучаются случаи квадратичного и кругового поля. Вводится понятие алгебры кватернионов.

Заключительный пятый раздел выступает введением в аналитическую теорию чисел. Дается определение характеров и L-функций Дирихле, доказывается теорема Дирихле о распределении простых чисел в арифметических прогрессиях. Вводится понятие дзета-функции Дедекинда, Обзорно приводятся результаты для числа классов идеалов числового поля.

Наименование разделов (тем) дисциплины	**Содержание разделов (тем) дисциплин**
Раздел I. Элементарная теория чисел Источники: [2, главы 1-5], [1]	
Тема 1. Простые числа	Делимость в кольце целых чисел, НОД, НОК, Алгоритм Евклида. Однозначное разложение целых чисел на простые множители. Бесконечность числа простых чисел. Мультипликативные функции, функции Эйлера и Мёбиуса. Формула обращения Мёбиуса. Неравенства Чебышева.
Тема 2. Сравнения	Сравнения и их свойства. Полная и приведенная система вычетов.

	Число решений линейного сравнения. Теоремы Эйлера и Ферма. Китайская теорема об остатках. Повторение основных определений алгебры: группа, кольцо, идеал, фактор-группа и фактор-кольцо, поле. Кольцо классов вычетов (определения и свойства выше на языке колец). Делители нуля. Кольцо многочленов над любым полем. Однозначность разложения в кольце многочленов.
Тема 3. Первообразные корни	Теорема Лагранжа (число корней многочлена над произвольным полем не превосходит степени многочлена). Группа единиц кольца вычетов по модулю простого. Структура группы единиц кольца вычетов по произвольному модулю. Первообразные корни и индексы. Степенные вычеты.
Тема 4. Квадратичные вычеты	Квадратичные вычеты и невычеты. Символ Лежандра, символ Якоби, их свойства. Теорема Вильсона и ее обобщение. Лемма Гаусса. Квадратичный закон взаимности. Равномерное распределение последовательностей mod n (обзорно).
Раздел II. Конечные поля Источники: [5, глава I], [2, глава 7], [4, глава I], [6, главы 2-3]	
Тема 5. Конечные поля. Соответствие Галуа	Кольцо многочленов $\mathbb{F}_p[x]$. Количество неприводимых многочленов над $\mathbb{F}_p$. Конечное поле $\mathbb{F}_q$ как фактор-кольцо кольца многочленов. Цикличность мультипликативной группы $\mathbb{F}_q$. $\mathbb{F}_q/\mathbb{F}_p$ как алгебраическое расширение. Автоморфизм Фробениуса. Цикличность группы Галуа конечного поля. Соответствие Галуа для башни конечных полей. Простота расширения $\mathbb{F}_q/\mathbb{F}_p$.
Тема 6. Корни из единицы. Круговой многочлен.	Круговой многочлен, круговое поле. Цикличность группы корней из единицы. Примитивные корни из единицы. Произведение круговых многочленов. Разложение кругового многочлена над конечным полем. Число неприводимых многочленов над конечным полем. Факты о неприводимых многочленах. Критерий неприводимости Эйзенштейна.
Тема 7. Норма и след. Характеры. Суммы Гаусса.	Норма и след, базовые свойства. Критерии тривиальности нормы и следа элемента конечного поля. Норма и след как коэффициенты минимального многочлена. Абсолютные и относительные норма и след. Характеры абелевых групп. Двойственная группа. Свойства ортогональности. Аддитивные и мультипликативные характеры

	конечного поля. Суммы Гаусса. Связь тригонометрических сумм с числом решений уравнений в конечных полях.
Тема 8. Тригонометрические суммы. Уравнения над конечными полями	Теоремы Варинга и Шевалле. Суммы характеров. Суммы Якоби, применение для числа решений уравнений. Неполные суммы характеров. Теорема Виноградова-Пойя, гипотезы Виноградова, Теорема Берджесса (без доказательства).
Тема 9. Дзета функция Артина, соотношение Хассе-Дэвенпорта	Дзета функция Артина, критерий рациональности. Элементы алгебраической геометрии над конечным полем: аффинное и проективное пространства, уравнения как гиперповерхности. Дзета функция одной гиперповерхности (форма стемени m) и её рациональность. Соотношение Хассе-Дэвенпорта для сумм Гаусса.
Раздел III. p-адические числа Источники: [3, глава I], [4, глава II], [7, главы 1-4]	
Тема 10. p-адические числа: элементарное определение и свойства	Элементарное определение кольца и поля p-адических чисел. Единицы кольца $\mathbb{Z}_p$. p-показатель и p-адическая метрика. Свойства вложения $\mathbb{Q}$ в $\mathbb{Q}_p$. Делимость и сравнения в $\mathbb{Z}_p$. Сходимость последовательностей и рядов p-адических чисел.
Тема 11. Аксиоматическое определение поля p-адических чисел, метризованные поля	Метризованные поля, пополнение по метрике, теорема о существовании и единственности пополнения метризованного поля (без доказательства). Эквивалентность метрик. Метрики поля рациональных чисел, Теорема Островского. Некоторые топологические свойства связанные с неархимедовыми метриками.
Тема 12. Лемма Гензеля, сравнения и кольцо целых p-адических чисел	Несколько вариантов формулировки Леммы Гензеля. Связь разрешимости сравнений по модулю степени простого с разрешимостью в поле p-адических чисел. Оценка числа решений сравнения по модулю степени простого. Теорема Минковского-Хассе и локально-глобальный принцип (обзорно).
Раздел IV. Числовые поля Источники: [2, главы 9,12-13], [3, глава III], [8, главы 2-5], [9, параграфы I.4, II.7], [10, глава 2]	
Тема 13. Кольцо целых гауссовых чисел, числовые поля	Однозначность разложения на множители в кольцах $\mathbb{Z}[i]$, $\mathbb{Z}[\omega]$. Кубический и биквадртичный характеры. Высшие законы взаимности. Суммы двух квадратов, суммы четырёх квадратов. Кватернионы.
Тема 14. Делимость в кольцах целых алгебраических чисел	Числовое поле. Норма, след, дискриминант. Порядки и кольца алгебраических целых чисел, Дедекиндовы кольца. Однозначность разложения в кольце алгебраических целых чисел. Элементы теории

	Галуа числовых полей (обзорно). Применение теории Галуа к разложению на простые идеалы в башнях полей и колец.
Тема 15. Квадратичное поле и круговое поле	Квадратичное числовое поле $\mathbb{Q}(\sqrt{d})$ и его кольцо целых. Порядки в квадратичном поле. Разложимость на простые идеалы. Связь с квадратичными формами. Число классов идеалов квадратичного поля (обзорно). Круговое поле $\mathbb{Q}(\zeta_m)$, простые идеалы соответствующего кольца целых. Приложения для кругового многочлена.
Раздел V. Теорема Дирихле Источники: [4, Глава VI], [2, глава 16], [3, глава V], [8, главы 7-8]	
Тема 16. Ряды Дирихле	Характеры Дирихле. Ряды Дирихле. Аналитическое продолжение. Дзета функция Римана. Асимптотический закон распределения простых чисел (обзорно).
Тема 17. Распределение простых чисел арифметической прогрессии	Теорема Дирихле о распределении простых чисел в арифметической прогрессии. L-функции и производящие функции. Дзета функция Дедекинда. Связь с числом классов идеалов числового поля.

5.3. Примеры задач для семинаров дисциплины

Наименование разделов (тем) дисциплины	**Примеры задач и упражнений**
Раздел I. Элементарная теория чисел	
Тема 1. Простые числа	**Задачи** 1. Пусть $a, b, c \in \mathbb{Z}$. Докажите что уравнение $ax + by = c$ имеет решение в целых числах $\Leftrightarrow (a, b)\|c$. 2. Докажите, что в кольце $\mathbb{Z}$ каждый идеал является главным. 3. Используя предыдущее упражнение, исследуйте вопрос разрешимости уравнения$ax_1 + ax_2 + \cdots + ax_n = c$ в целых числах. 4. Докажите, что $\mathrm{ord}_p(a + b) \geq \min(\mathrm{ord}_p a, \mathrm{ord}_p b)$, причем равенство выполняется если $\mathrm{ord}_p a \neq \mathrm{ord}_p b$. 5. Докажите, что $\mathrm{ord}_p n! = [n/p] + [n/p^2] + [n/p^3] + \cdots$

	6. Пусть $\tau(n) = \sum_{d\|n} 1$, $\sigma(n) = \sum_{d\|n} d$ – число и сумма делителей. Докажите, что $\tau(n)$ и $\sigma(n)$ – мультипликативные функции и что если $n = \prod_{i=1}^{k} p^{a_i}$ то $\tau(n) = \prod_{i=1}^{k}(a_i + 1)$, $\sigma(n) = \prod_{i=1}^{k} \frac{p_i^{a_i+1}-1}{p_i-1}$ 7. Пусть $\alpha \in \mathbb{R}$, $c \in \mathbb{Z}_{>0}$. Докажите что для целой части справедливо равенство $[\frac{[\alpha]}{c}] = [\frac{\alpha}{c}]$. **SageMath** ● Основные теоретико-числовые функции: НОД, НОК, разложение на множители, функции Эйлера, Мёбиуса, целая и дробная часть, число и сумма делителей, число простых чисел в интервале.
Тема 2. Сравнения	**Задачи:** 1. Используя сравнимость $\mathrm{mod}\, n$, докажите что уравнения $3x^2 + 2 = y^2$ и $3x^3 + 2 = y^3$ не разрешимы в целых числах. 2. Докажите, что $(p-1)! \equiv -1 (\mathrm{mod}\, p)$. 3. Докажите, что p делит биномиальные коэффициенты C_p^k при $1 \le k \le p-1$, выведите из этого, что $(a+1)^p = a^p + 1 (\mathrm{mod}\, p)$. 4. Пусть p, q – различные нечетные простые такие что $p-1 \mid q-1$, докажите что если $(n, pq) = 1$ то $n^{q-1} \equiv 1 (\mathrm{mod}\, pq)$ 5. Пусть $f(x) \in \mathbb{Z}[x]$, $n = \prod_{i=1}^{k} p^{a_i}$. Докажите, что $f(x) \equiv 0 (\mathrm{mod}\, n) \Leftrightarrow f(x) \equiv 0 (\mathrm{mod}\, p^{a_i})$, $1 \le i \le k$. Докажите, что при этом если N – число решений сравнения $f(x) \equiv 0 (\mathrm{mod}\, n)$, то $N = \prod_{i=1}^{k} N_i$, где N_i – число решений сравнения $f(x) \equiv 0 (\mathrm{mod}\, p^{a_i})$, $1 \le i \le k$. 6. Сформулируйте и докажите китайскую теорему об остатках для произвольной области главных идеалов. 7. Пусть a, b, m – целые, $m > 1$, $(a, m) = 1$, x пробегает полную систему вычетов, а ξ – приведенную $\mathrm{mod}\, m$.

	Докажите, что $\sum_x \left\{\frac{ax+b}{m}\right\} = \frac{1}{2}(m-1)$, $\sum_\xi \left\{\frac{a\xi}{m}\right\} = \frac{1}{2}\phi(m)$. ($\{\cdot\}$ – дробная часть числа, $\{x\} = x - [x]$). **SageMath:** ● Модулярная арифметика. Решение систем линейных сравнений. Коммутативные кольца и их идеалы. Кольца многочленов, арифметика в кольце многочленов, разложение многочленов на множители.
Тема 3. Первообразные корни	**Задачи:** 1. Докажите, что 3 – первообразный корень простого числа вида $p = 2^n + 1$. 2. Пусть p – простое, a – первообразный корень $\bmod p^n$. Докажите, что тогда a – первообразный корень $\bmod p$. 3. Пусть p – простое, $p \equiv 1 \pmod 4$. Докажите что a – первообразный корень $\bmod p \Leftrightarrow -a$ – первообразный корень $\bmod p$. 4. Пусть p – простое, $p \equiv 3 \pmod 4$. Докажите что a – первообразный корень $\bmod p \Leftrightarrow -a$ имеет индекс (порядок) $(p-1)/2$. 5. Пусть q – простое вида $2p+1$, где p – простое. Докажите, что первообразный корень $\bmod q$ есть 2 если $p \equiv 1 \pmod 4$ и -2 если $p \equiv 3 \pmod 4$. 6. Пусть g – первообразный корень $\bmod p$, $d \mid (p-1)$. Докажите, что $g^{(p-1)/d}$ имеет индекс (порядок) d, а также что a является d-ой степернью $\Leftrightarrow a \equiv g^{kd} \pmod p$ для некоторого k. 7. Пусть G – конечная циклическая группа порядка n, g – образующая G. Докажите, что все образующие имеют вид g^k, $(k, n) = 1$. 8. Пусть G – конечная абелева группа, a, b – элементы порядков m, n соответственно. Докажите, что если $(m, n) = 1$ то порядок элемента ab равен mn. **SageMath:**

	• Поиск корней многочленов. Определение первообразных корней. Решение степенных сравнений. Псевдопростые числа, числа Кармайкла.
Тема 4. Квадратичные вычеты	**Задач:** 1. Пусть p – простое, $(a,p) = 1$. Докажите что число решений сравнения $ax^2 + bx + c \equiv 0 \pmod p$ равно $1 + \left(\frac{b^2-4ac}{p}\right)$. 2. Докажите, что $\sum_{x \bmod p} \left(\frac{x}{p}\right) = 0$, а также что если $(a,p) = 1$ то $\sum_{a \bmod p} \left(\frac{ax+b}{p}\right) = 0$. 3. Используя замену переменных, докажите что число решений сравнения $x^2 - y^2 \equiv a \pmod p$ равно $p - 1$ если $(a,p) = 1$ и $2p - 1$ если $p \mid a$. Выразите число решений этого сравнения через сумму с символом Лежандра. Используя эти выражения, найдите значение для $\sum_{y \bmod p} \left(\frac{y^2+a}{p}\right)$. 4. Пусть $r_1, \cdots, r_{(p-1)/2}$ – квадратичные вычеты в промежутке $[1; p]$. Докажите что их произведение $\equiv 1\ (p)$ если $p \equiv 3\ (4)$ и $\equiv -1\ (p)$ если $p \equiv 1\ (4)$. 5. Пусть $f(x) \in \mathbb{Z}[x]$. Будем говорить что простое p делит $f(x)$, если $\exists n \in \mathbb{Z}$ такое что $p \mid f(n)$. Опишите простые делители многочленов $x^2 + 1$ и $x^2 - 1$. Докажите, что если p делит $x^4 - x^2 + 1$, то $p \equiv 1 \pmod{12}$. 6. Пусть D – целое положительное нечетное и свободное от квадратов число. Докажите, что $\exists b \in \mathbb{Z},\ (b,D) = 1$ таке что $(b/D) = -1$. Докажите также, что $\sum_a{}' \left(\frac{a}{D}\right) = 0$ где суммирование берется по приведенной системе вычетов $\bmod D$. 7. Пусть p – нечетное простое. Докажите, что $\left(\frac{2}{p}\right) = \prod_{j=1}^{(p-1)/2} 2\cos\frac{2\pi j}{p}$, а также что если $p > 3$ то $\left(\frac{3}{p}\right) = \prod_{j=1}^{(p-1)/2} (3 - 4\sin^2\frac{2\pi j}{p})$.

	SageMath: ● Вычисление символов Лежандра и Якоби. Решение некоторых сравнений. Поиск представлений целого числа в виде суммы квадратов, решение других диофантовых уравнений. Численные эксперименты с числом квадратичных вычетов и невычетов в заданных интервалах. Статистические тесты равномерного распределения некоторых последовательностей.
Раздел II. Конечные поля	
Тема 5. Конечные поля. Соответствие Галуа	**Задачи:** 1. Докажите, что многочлен $x^2 + 1$ неприводим над $\mathbb{F}_{11}$, определите количество элементов в поле $\mathbb{F}_{11}[x]/(x^2 + 1)$. Докажите что многочлен $x^2 + x + 4$ также неприводим над $\mathbb{F}_{11}$ и что поле $\mathbb{F}_{11}[x]/(x^2 + 1)$ изоморфно полю $\mathbb{F}_{11}[x]/(x^2 + x + 4)$. 2. Докажите, что в конечном поле $\mathbb{F}_q$ справедливы соотношения: 1) $\sum_{\alpha \in \mathbb{F}_q} \alpha = 0$, при $q \neq 2$ 2) $\prod_{\alpha \in \mathbb{F}_q} \alpha = -1$ (аналог теоремы Вильсона). 3. Докажите, что в поле простой характеристики p спрпаедливо равенство: $\left(\sum_{j=1}^{m} \alpha_j\right)^{p^n} = \sum_{j=1}^{m} \alpha_j^{p^n}$. 4. Пусть функция $L(n)$ определена равенством $1 + b^n = b^{L(n)}$, для $b^n \neq -1$ ($L(n)$ – так называемый логарифм Якоби). Докажите что $b^n + b^m = b^{m+L(n-m)}$, если $L(n), L(m)$ определены. 5. Пусть F – произвольное поле. Докажите что всякая конечная подгруппа мультипликативной группы F^* является циклической. 6. Пусть F – произвольное поле. Докажите, что если F^* является циклической то F – конечное поле. 7. Пусть F – конечное поле, H – подгруппа мультипликативной группы F^*. Докажите что $H \cup \{0\}$ является подполем $F \Leftrightarrow$

	порядок F^* равен либо 1 либо простому числу вида $2^p - 1$, где p – простое. **SageMath:** ● Количество элементов в конечных полях. Примитивные элементы, неприводимость многочленов над конечными полями. Многочлены Конвея. Алгебраическое замыкание конечного поля.
Тема 6. Корни из единицы. Круговой многочлен.	**Задачи:** 1. Докажите что для каждого элемента из $\mathbb{F}_q$ $(q = p^n)$ существует только один корень p-ой степени из единицы. 2. Пусть $q \equiv 1 \pmod n$. Докажите, что для $\alpha \in \mathbb{F}_q$ уравнение $x^n = \alpha$ либо не имеет решений, либо имеет n решений. Докажите также, что множество $\{\alpha \in \mathbb{F}_q^* : x^n = \alpha$ – разрешимо$\}$ является подгруппой $\mathbb{F}_q^*$ из $(q-1)/n$ элементов. 3. Пусть $q \equiv 1 \pmod n$, $E/\mathbb{F}_q$ – расширение степени $[E:\mathbb{F}_q] = n$. Докажите, что для $\alpha \in \mathbb{F}_q^*$ уравнение $x^n = \alpha$ имеет n решений в E. 4. Пусть E/F – расширение конечных полей степени $[E:F] = 3$. Докажите, что если $\alpha \in F$ не является квадратом в F, то α также не является квадратом в E. 5. Пусть $q > 2$. Докажите, что $\alpha \in \mathbb{F}_q^*$ является квадратом $\Leftrightarrow$ $\alpha^{(q-1)/2} = 1$. Обобщите результат для любой степени k: $\alpha \in \mathbb{F}_q^*$ является k-ой $\Leftrightarrow \alpha^{(q-1)/d} = 1$, где $d = (q-1, k)$. 6. Пусть $\alpha \in \mathbb{F}_q$ – элемент порядка m, $q = p^n$, ν – индекс (показатель) числа p по модулю m. Докажите, что многочлен $f(x) = \prod_{j=0}^{\nu-1}(x - \alpha^{p^j})$ является неприводимым в кольце $\mathbb{F}_p[x]$. 7. Пусть F – произвольное поле, $n > 1$. Докажите что многочлен $x^{n-1} + x^{n-2} + \cdots + x + 1$ неприводим над K только если n – простое число.

	SageMath: ● Элементы линейной алгебры: матрицы, векторные пространства и модули. Решение систем линейных уравнений. Идеалы кольца многочленов над конечным полем. Идемпотентные многочлены и идеалы. Круговой многочлен и его разложение.
Тема 7. Норма и след. Характеры. Суммы Гаусса.	**Задачи:** 1. Пусть $q = p^n$. Докажите, что для каждого $\alpha \in \mathbb{F}_p^*$ уравнение $\mathrm{N}\, x = \alpha$ имеет $(p^n - 1)/(p - 1)$ решений, а также что для каждого $\beta \in \mathbb{F}_p$ уравнение $\mathrm{Tr}\, x = \beta$ имеет p^{n-1} решений. 2. Пусть $q = p^n$, $p \neq 2$. Определим аналог символа Лежандра для $\mathbb{F}_q$: $\left(\frac{\alpha}{p}\right) = 1$, если $\alpha \neq 0$ – квадрат в $\mathbb{F}_q$; $\left(\frac{\alpha}{p}\right)$=-1, если $\alpha \neq 0$ не является квадратом в $\mathbb{F}_q$; $\left(\frac{0}{p}\right) = 0$. Докажите следующие свойства: 1) $\forall \alpha, \beta \in \mathbb{F}_q \left(\frac{\alpha\beta}{q}\right) = \left(\frac{\alpha}{q}\right)\left(\frac{\beta}{q}\right)$; 2) $\sum_{\alpha \in \mathbb{F}_q} \left(\frac{\alpha}{q}\right) = 0$; 3) $\left(\frac{\alpha}{q}\right) = \left(\frac{\mathrm{N}\,\alpha}{p}\right)$ – обычный символ Лежандра $\mathrm{mod}\, p$. 3. Пусть $f(x) = ax^2 + bx + c \in \mathbb{F}_q[x]$, $q = p^n$, $p \neq 2$, обозначим $d = b^2 - 4ac$ дискриминант этого многочлена. Докажите, что $\sum_{x \in \mathbb{F}_q} \left(\frac{f(x)}{q}\right) = \left(\frac{a}{q}\right)(q - 1)$, если $d = 0$ и =-$\left(\frac{a}{q}\right)$, если $d \neq 0$. Получите из этого результата формулу для числа решений уравнения $ax^2 + by^2 = \alpha$ в элементах поля $\mathbb{F}_q$. 4. Пусть F – поле $f(x), g(x) \in F[x]$, $f(x) = a_0 x^m + \cdots = a_0 \prod_{j=1}^{m} (x - \alpha_j)$, $g(x) = b_0 x^n + \cdots = b_0 \prod_{k=1}^{n} (x - \beta_k)$. Положим $D(f) = a_0^{2(m-1)} \prod_{j<i} (\alpha_j - \alpha_i)^2$ – дискриминант многочлена f, $R(f, g) = a_0^{\,n} b_0^{\,m} \prod_j \prod_j (\alpha_j - \beta_k)^2$ – результант многочленов f, g

	. Докажите следующие свойства: 1) $R(g,f) = (-1)^{mn}R(f,g)$; 2) если $g = fh + r$ то $R(f,g) = a_0^{n-deg\,r}R(f,r)$; 3) если $f = f_1 f_2$, то $R(f,g) = R(f_1,g)R(f_2,g)$; 4) $R(f,g) = a_0^n \prod_{j=1}^{m} g(\alpha_j)$ 5. Пусть $p > 2$ – простое, $\tau(p) = \sum_{x=0}^{p-1} e_p(x^2)$ – сумма Гаусса. $A = \left(e_p(st)\right)_{0\le s,t\le p-1}$ – матрица. Докажите, что: 1) если $\lambda_1, \cdots, \lambda_p$ – характеристические числа матрицы A, то $\sum_{k=1}^{p} \lambda_k = \tau(p)$; 2) характеристический многочлен матрицы A^2 имеет вид: $(t-p)^{(p+1)/2}(t+p)^{(p-1)/2}$; 3) для определителя матрицы A справедливо $det\, A = i^{p(p-1)/2}p^{p/2}$. 6. Пусть G – конечная абелева группа, H – собственная подгруппа, $g \in G$, $g \notin H$. Докажите, что существует характер χ группы G такой что $\chi(g) \neq 1$ и $\forall h \in H\ \chi(h) = 1$. 7. Пусть G – конечная абелева группа, $m > 0$ – целое. Докажите, что $g \in G$ является m-ой степенью в $G \Leftrightarrow \forall$ характера χ степени m ($\chi^m = \varepsilon$) выполняется $\chi(g) = 1$. **SageMath:** ● Базисы Грёбнера. Дискриминант и результант многочленов. Характеры и представления групп.
Тема 8. Тригонометрические суммы. Уравнения над конечными полями	**Задачи:** 1. Пусть χ – нетривиальный мультипликативный характер поля $\mathbb{F}_p$, ρ – характер порядка 2. Докажите, что $\sum_{t\in\mathbb{F}_p} \chi(1-t^2) = J(\chi,\rho)$. 2. Пусть χ – нетривиальный мультипликативный характер поля $\mathbb{F}_p$. Докажите, что $\sum_{t\in\mathbb{F}_p} \chi(1-t^m) = \sum_{\lambda} J(\chi,\lambda)$, где суммирование берется по всем характерам λ таким что $\lambda^m = \varepsilon$

	, где ε – тривиальный характер. Выведете отсюда, что $\left\| \sum_{t \in \mathbb{F}_p} \chi(1 - t^m) \right\| \leq (m-1)p^{1/2}$. 3. Пусть χ – нетривиальный мультипликативный характер поля $\mathbb{F}_p$, ρ – характер порядка 2. Докажите, что если $k \in \mathbb{F}_p^*$, то $\sum_{t \in \mathbb{F}_p} \chi(t(k-t)) = \chi(\frac{k^2}{4}) J(\chi, \rho)$. 4. Пусть χ – мультипликативный характер, такой что $\chi^2 \neq \varepsilon$, ρ – характер порядка 2. Докажите, что $\tau(\chi)^2 = \frac{1}{\chi(2)^2} J(\chi, \rho)\tau(\chi^2)$. А также, что $J(\chi, \chi) = \frac{1}{\chi(2)^2} J(\chi, \rho)$. 5. Пусть $p \equiv 1\ (3)$ – простое, χ – характер порядка 3, ρ – символ Лежандра. Докажите, что для числа решений уравнения справедливо $N(y^2 = 1 - x^3) = p + \sum_{x \in \mathbb{F}_p} \rho(1 - x^3)$ $= p + 2\mathrm{Re}\, J(\chi, \rho)$. 6. Пусть $f: \mathbb{F}_q \to \mathbb{C}$, определим $\widehat{f}(s) = \frac{1}{q} \sum_{t \in \mathbb{F}_q} f(t)\, \overline{\psi(st)}$. Докажите, что $f(t) = \frac{1}{q} \sum_{s \in \mathbb{F}_q} \widehat{f}(s)\psi(st)$. 7. Пусть $p > 60$, χ – нетривиальный мультипликативный характер $\bmod p$, M, Q – целые, $0 < M < M + Q < p$. Докажите, что $\sum_{x=M}^{M+Q-1} \chi(x) < p^{1/2}(\log p - 1)$. **SageMath:** ● Поиск решений уравнений над конечными полями. Численные эксперименты с оценками тригонометрических сумм.
Тема 9. Дзета функция Артина, соотношение Хассе-Дэвенпорта	**Задачи:** 1. Докажите, что проективная n-мерная гиперплоскость в $\mathbb{P}^n(\mathbb{F}_q)$ (т.е. Гиперповерхность, заданная однородным многочленом степени 1) имеет столько точек сколько $n-1$-мерное проективное пространство $\mathbb{P}^{n-1}(\mathbb{F}_q)$.

	2. Рассмотрим кольцо многочленов $\mathbb{F}_q[x_0, \cdots, x_n]$,определим операторы $\frac{\partial}{\partial x_i}$ формальных производных (например, для $f(x) = a_0 x^n + \cdots + a_{n-1}x + a_n$ по определению $\frac{\partial}{\partial x} f = a_0 n x^{n-1} + \cdots + a_{n-1}$). Пусть $f \in \mathbb{F}_q[x_0, \cdots, x_n]$ – однородный многочлен степени m. Докажите, что $\sum_{i=0}^{n} x_i \frac{\partial}{\partial x_i} f = mf$. 3. Пусть $q = p^n$, $f \in \mathbb{F}_q[x_0, \cdots, x_n]$ – однородный многочлен степени m, $(m, p) = 1$. Докажите, что если для $\bar{a} = (a_0, \cdots, a_n) \in \mathbb{P}^n(\mathbb{F}_q)$ при всех i выполняется $\frac{\partial}{\partial x_i} f(\bar{a}) = 0$, то $f(\bar{a}) = 0$. Такая точка $\bar{a} \in \mathbb{P}^n(\mathbb{F}_q)$ называется особой точкой гиперповерхности $f = 0$. 4. Пусть $q = p^n$,$(m, p) = 1$. Докажите, что гиперповерхность $a_0 x_0^m + \cdots + a_n x_n^m = 0$ не имеет особых точек в $\mathbb{P}^n(\mathbb{F}_q)$. 5. Пусть $q = p^n$, $p \neq 2$. Рассмотрим кривую $ax^2 + bxy + cy^2 = 1$, $a, b, c \in \mathbb{F}_q^*$. Докажите, что если $d = b^2 - 4ac$ не является квадратом в $\mathbb{F}_q$, то не существует бесконечно удаленных точек на кривой в $\mathbb{P}^n(\mathbb{F}_q)$, а если d – квадрат, то существует одна или две бесконечно удаленные точки, в зависимости от обращения d в ноль . При этом если $d = 0$, то бесконечно удаленная точка является особой точкой заданной кривой. 6. Выпишите дзета-функцию кривой $x_0 x_1 - x_2 x_3 = 0$ над $\mathbb{F}_p$. 7. Покажите, что на кривой $x_0^3 + x_1^3 + x_2^3 = 0$ в $\mathbb{P}^2(\mathbb{F}_4)$ лежит девять точек. Выпишите дзета-функцию этой кривой. 8. Выпишите дзета-функцию кривой $y^2 = x^3 + x^2$ над $\mathbb{F}_p$. **SageMath:** ● Численные эксперименты с оценками тригонометрических сумм (продолжение). Определение количества точек на алгебраических кривых и поверхностях над конечными полями. Решение рекуррентных соотношений.
Раздел III. p-адические числа	

Тема 10. p-адические числа: элементарное определение и свойства	**Задачи:** 1. Пусть $\xi = \sum_{n=0}^{\infty} a_n p^n \in \mathbb{Q}_p$. Выпишите разложение числа -ξ. 2. Пусть последовательность (x_n) определена как $x_n = 1 + p + \cdots + p^{n-1}$. Докажите, что в $\mathbb{Q}_p$ $\lim_{n\to\infty} x_n = 1/(1-p)$. 3. Пусть $p \neq 2$, c – квадратичный вычет $\bmod p$. Докажите, что существует два различных p-адических числа $\alpha, \beta \in \mathbb{Q}_p$ таких что $\alpha^2 = \beta^2 = c$. 4. Пусть $c \in \mathbb{Z}$. Докажите, что последовательность (c^{p^n}) сходится в $\mathbb{Q}_p$, при этом для $\gamma = \lim_{n\to\infty} c^{p^n}$ имеем $\gamma \equiv c \pmod p$, $\gamma^{p-1} = 1$. 5. Используя результат предыдущей задачи, докажите что в $\mathbb{Q}_p[t]$ многочлен $t^{p-1} - 1$ раскладывается на линейные множители. 6. Докажите, что для $\xi \in \mathbb{Q}_p \cap \mathbb{Q}$, $\xi \neq 0$ представление $\xi = \sum_{n=0}^{\infty} a_n p^n$ имеет периодические коэффициенты (начиная с некоторого номера k_0, т.е. $\exists m \, \forall k \geq k_0 \; a_{k+m} = a_k$). Обратно, всякий такой ряд представляет рациональное число. 7. Докажите p-адический критерий Эйзенштейна: пусть $f \in \mathbb{Z}_p[x]$, $f(x) = a_0 x^n + \cdots + a_n$ – неприводим, если $p \nmid a_0, p \mid a_i \; 1 \leq i \leq n, p \nmid a_n$. **SageMath:** ● Поле и кольцо p-адических чисел. Разложение p-адических чисел с заданной точностью.
Тема 11. Аксиоматическое определение поля p-адических чисел, метризованные поля	**Задачи:** 1. Докажите, что если характеристика поля k равна $p > 0$, то всякая метрика поля является неархимедовой.

	2. Пусть (k, φ) – метризованное поле. Докажите что если выполняется свойство $\varphi(x) \leq 1 \Rightarrow \varphi(x \pm 1) \leq 1$, то φ – неархимедова метрика. 3. Пусть (k, φ) – метризованное поле, $d(x, y) = \varphi(x - y)$ – соответствующая функция расстояния. Докажите что k – топологическое поле, т.е. все операции поля k непрерывны по расстоянию d. 4. Докажите, что $(\mathbb{Z}_2, \lvert \cdot \rvert_2)$ гомеоморфно Канторову множеству $(C, \lvert \cdot \rvert)$ в $\mathbb{R}$. 5. Докажите, что $\forall p$ $(\mathbb{Z}_p, \lvert \cdot \rvert_p)$ гомеоморфно $(\mathbb{Z}_2, \lvert \cdot \rvert_2)$. 6. Пусть k – поле, $k(t)$ – поле рациональных функций, $k(t) = \left\{\frac{f(t)}{g(t)} : f, g \in k[x],\ g \neq 0\right\}$. Каждую ненулевую рациональную функцию можно представить виде $\frac{f(t)}{g(t)} = t^m \frac{f_1(t)}{g_1(t)}$, $f_1(0) \neq 0$, $g_1(0) \neq 0$, положим $\varphi(f/g) = \rho^m$, $0 < \rho < 1$, $\varphi(0) = 0$. Докажите, что φ является метрикой поля $k(t)$. 7. В условиях предыдущей задачи, докажите, что пополнение поля $k(t)$ по метрике φ изоморфно полю формальных степенных рядов. **SageMath:** ● Визуализация кольца целых р-адических чисел. Формальные ряды, поле рациональных функций, Аппроксимация Паде.
Тема 12. Лемма Гензеля, сравнения и кольцо целых р-адических чисел	**Задачи:** 1. Докажите, что если $(m, p) = 1$, $\varepsilon \in \mathbb{Z}_p$ – единица, $\varepsilon \equiv 1 \pmod{p}$, то ε является m-ой степенью в $\mathbb{Q}_p$. 2. Пусть $m = p^\delta m_0$, $(m_0, p) = 1$, $\varepsilon \in \mathbb{Z}_p$ – единица, $\varepsilon \equiv 1 \pmod{p^{2\delta+1}}$. Докажите что ε является m-ой степенью в $\mathbb{Q}_p$. 3. Докажите, что единица $\varepsilon \in \mathbb{Z}_2$ является квадратом $\Leftrightarrow$ $\varepsilon \equiv 1\ (8)$. 4. Докажите, что порядок группы $\mathbb{Q}_2/(\mathbb{Q}_p^*)^2$ равен 8. Найдите систему представителей для этой группы.

	5. Докажите, что в $\mathbb{Q}_2$ квадратичная форма $F = F_0 + 2F_1$ (в обозначениях лекции) представляет 0 (нетривиально) ⇔ разрешимо сравнение $F(X) \equiv 0\ (16)$ с нечетным значением хотя бы одного x_i. 6. Исследуйте верно ли утверждение: многочлен $f \in \mathbb{Z}[x]$ неприводим в $\mathbb{Q}[x] \Leftrightarrow f$ неприводим в $\mathbb{Q}_p[x]\ \forall p \leq \infty$. 7. Пусть $F \in \mathbb{Z}_p[x_1, \cdots, x_n]$, N_m – число решений сравнения $F(x_1, \cdots, x_n) \equiv 0\ (\mathrm{mod}\ p^m)$, составим ряд $\sum_{m=0}^{\infty} N_m t^m$ (так называемый ряд Пуанкаре). Докажите, что ряд Пуанкаре для $F = \varepsilon_1 x_1 + \cdots \varepsilon_n x_n$, где ε_i – p-адические единицы, является рациональной функцией. **SageMath:** ● Кольцо многочленов многих переменных, его арифметика. Системы уравнений с многочленами от нескольких переменных. Поиск корней рациональных и вещественных корней многочленов. Кольцо многочленов с p-адическими коэффициентами.
Раздел IV. Числовые поля	
Тема 13. Кольцо целых гауссовых чисел, числовые поля	**Задачи:** 1. Докажите, что $(1 + i)^2 \mid 2$ в $\mathbb{Z}[i]$, а $(1 - \omega)^2 \mid 3$ в $\mathbb{Z}[\omega]$. 2. В кольце $\mathbb{Z}[\omega]$ найдите ассоциированные простые элементы для $1 - 2\omega, -7 - 3\omega, 3 - \omega$. 3. Пусть $m, n \in \mathbb{Z}$. Докажите, что m, n взаимно просты в $\mathbb{Z}[i] \Leftrightarrow$ m, n взаимно просты в $\mathbb{Z}$. 4. Докажите, что $a + bi \in \mathbb{Z}[i]$ – единица кольца $\mathbb{Z}[i] \Leftrightarrow$ $\mathrm{N}(a + bi) = a^2 + b^2 = 1$, а $a + b\omega \in \mathbb{Z}[\omega]$ – единица кольца $\mathbb{Z}[\omega] \Leftrightarrow \mathrm{N}(a + b\omega) = a^2 - ab + b^2 = 1$. Опишите все единицы колец $\mathbb{Z}[i]$ и $\mathbb{Z}[\omega]$. 5. Пусть π – простой элемент в $\mathbb{Z}[\omega]$. Докажите, что класс вычетов α в $\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$ является кубом ⇔ $\alpha^{(\mathrm{N}\pi-1)/3} \equiv 1\ (\mathrm{mod}\ \pi)$. Выведете из этого, что число кубов в $\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$ равно $(\mathrm{N}\pi - 1)/3$.

	6. Пусть $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2}: a, b \in \mathbb{Z}\}$, $\mathsf{N}(a + b\sqrt{2}) = a^2 + 2b^2$, докажите, что $\mathbb{Z}[\sqrt{2}]$ – Евклидово кольцо, причём ± 1 – единственные единицы. 7. Пусть $\mathbb{H}(\mathbb{Z})$ – алгебра кватернионов над $\mathbb{Z}$. Докажите, что следующие утверждения эквивалентны: 1) элемент $q \in \mathbb{H}(\mathbb{Z})$ обратим в $\mathbb{H}(\mathbb{Z})$; 2) $\mathsf{N}\, q = 1$; 3) $q \in \{\pm 1, \pm i, \pm j, \pm k\}$. **SageMath:** ● Числовые поля и порядки числовых полей. Символы степенных вычетов. Представление чисел суммами квадратов, решение некоторых диофантовых уравнений. Алгебра кватернионов.
Тема 14. Делимость в кольцах целых алгебраических чисел	**Задачи:** 1. Докажите, что $\mathbb{Z}[\sqrt{-5}]$ не содержит элементов нормы 2 и 3. Убедитесь, что $2 \cdot 3 = (1 + \sqrt{-5})(1 + \sqrt{5})$ – является примером неоднозначного разложения на простые элементы в кольце $\mathbb{Z}[\sqrt{-5}]$. 2. Пусть R – кольцо целых $\mathbb{Q}(\sqrt{d})$, $M > 0$. Докажите, что существует конечное число $\alpha \in R$ таких, что $\max(\alpha, \alpha') \leq M$, где α' – сопряженное к α. 3. Пусть $n \geq 1$ – целое. Докажите, что существует только конечное число целых алгебраических чисел α степени n таких, что $\lvert\alpha_j\rvert = 1\ \forall j$, α_j – сопряженные α, при этом все такие α являются корнями из единицы. 4. Вычислите дискриминант корня многочлена $x^3 + ax + b \in \mathbb{Q}[x]$ 5. Вычислите дискриминанты корней многочленов $x^n + ax + b$ и $x^n + ax^{n-1} + b \in \mathbb{Q}[x]$. 6. Пусть R – коммутативное кольцо. Докажите, что определитель Вандермонда для $a_1, \cdots a_n \in R$ равен $\prod_{1 \leq r < s \leq n} (a_s - a_r)$. 7. Пусть R – кольцо целых числового поля F. Докажите, что если дискриминант $\alpha_1, \cdots \alpha_n \in R$ свободен от квадратов, то $\alpha_1, \cdots \alpha_n$ образуют целый базис R. Примените это утверждение для кольца целых квадратичного поля $\mathbb{Q}(\sqrt{d})$.

	SageMath: ● Норма, след, дискриминант. Группа Галуа многочлена с рациональными коэффициентами. Базы данных числовых полей (NFDB, LMFDB).
Тема 15. Квадратичное поле и круговое поле	**Задачи:** 1. Докажите, что $1 + \sqrt{2}$ – единица в $\mathbb{Z}[\sqrt{2}]$, не являющаяся корнем из единицы. Используйте степени $1 + \sqrt{2}$ чтобы описать семейство решений диофантового уравнения $a^2 - 2b^2 = \pm 1$. 2. Пусть I – идеал в кольце $\mathbb{Z}[\sqrt{-3}]$, порожденный $2, 1 + \sqrt{-3}$. Докажите, что $I \neq (2)$, но $I^2 = 2I$, а также, что I – единственный простой идеал содержащий (2). 3. Докажите, что поля $\mathbb{Q}(\sqrt{m})$ попарно различны для m свободных от квадратов. 4. Пусть F – числовое поле, такое что $e^{2\pi i/n} \in F$ для некоторого $n \geq 3$. Докажите, что тогда $\forall \alpha \in F^* \ \mathrm{N}\alpha > 0$. 5. Докажите что квадратичное поле не может одновременно содержать $\sqrt{p}$ и $\sqrt{q}$ для двух различных простых p, q. 6. Докажите, что при $1 \leq j \leq p - 1 \frac{\sin(\pi j/p)}{\sin(\pi/p)}$ – единица в $\mathbb{Q}(e^{2\pi i/p})$. 7. Пусть p – простое, $p \equiv 3\ (4)$. Докажите, что $\mathbb{Q}(\sqrt{p}) \in \mathbb{Q}(e^{\pi i/2p})$. **SageMath:** ● Разложение на множители в порядках числовых полей. Представление целых чисел квадратичными формами. Число классов.
Раздел V. Теорема Дирихле	
Тема 16. Ряды Дирихле	**Задачи:** 1. Докажите, что 1) $\sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} = \frac{1}{\zeta(s)}$; 2) $\sum_{n=1}^{\infty} \frac{\sigma_a(n)}{n^s} = \zeta(s)\zeta(s-a)$.

	2. Пусть χ – нетривиальный характер $\mod 3$. Докажите, что $L(1,\chi) = \sum_{n=0}^{\infty} \frac{1}{(3n+1)(3n+2)}$. 3. Рассматривая $\Phi_m(x) \bmod p$ найдите алгебраическое доказательство существования бесконечного числа простых чисел в арифметической прогрессии $mk + 1$. 4. Пусть p – простое, $\tau(\chi)$ – сумма Гаусса для символа Лежандра $\chi(\cdot) = (\cdot/p), P = \prod_{(n/p)=-1} (1 - e^{2\pi i\, n/p}) \prod_{(r/p)=1} (1 - e^{2\pi i\, r/p})$. Докажите, что $P = e^{\tau(\chi)\, L(1,\chi)}$. 5. Пусть χ – характер Дирихле $\mod m$, $\chi(2) \neq 0$. Докажите, что $L(s,\chi) = (1 - 2^{-s}\chi(2))^{-1} \sum_{n=0}^{\infty} \frac{\chi(2n+1)}{(2n+1)^s}$. 6. Пусть p – простое, $p \equiv 3\ (4)$. Докажите, что $\sum_{x=1}^{p-1} \left(\frac{x}{p}\right) \sin\frac{2\pi x}{p} = \sqrt{p}$. 7. Пусть p – простое, $p \equiv 3\ (4)$. Докажите, равенства $\sum_{n\equiv 1(2)} \left(\frac{n}{p}\right)\frac{1}{n} = \frac{1}{\sqrt{p}} \sum_{t=1}^{p-1} \left(\frac{t}{p}\right) \sum_{m\equiv 1(2)} \frac{\sin(2\pi tm/p)}{m} = \frac{\pi}{2\sqrt{p}} \sum_{t=1}^{(p-1)/2} \left(\frac{t}{p}\right)$. **SageMath:** ● Характеры Дирихле. Вычисление значений специальных функций. Нули дзета-функции Римана. Численные эксперименты с оценкой сумм характеров Дирихле.
Тема 17. Распределение простых чисел арифметической прогрессии	**Задачи:** 1. Вычислите плотность распределения простых чисел $p \equiv 1 \pmod 3$. 2. Вычислите плотность распределения простых чисел p, которые раскладываются в произведение 4-х различных простых идеалов в кольце целых чисел поля $\mathbb{Q}(e^{2\pi i/5})$. 3. Используя теорему Дирихле, докажите, что $\forall$ конечной циклической группы G существует расширение Галуа поля рациональных чисел $\mathbb{Q}$ с группой автоморфизмов G. 4. Используя теорему Дирихле, докажите что круговой многочлен $\Phi_n(x) \in \mathbb{Q}[x]$ неприводим.

	5. Пусть $m \geq 2$, $(a, m) = 1$, f – порядок a в группе единиц $\mathrm{mod}\ m$. Докажите, что существует бесконечно много простых p таких, что $(p) = P_1 \cdots P_t$, $t = \varphi(m)/f$, P_i – различные простые идеалы в $\mathbb{Q}(e^{2\pi i/m})$. Вычислите плотность распределения таких простых чисел p. 6. Пусть K – числовое поле. Докажите, что ряд $\sum_P \frac{1}{\mathrm{N}(P)^s}$, ($P$ пробегает все простые идеалы поля K) сходится. Выведете отсюда сходимость произведения $\prod_P \left(1 - \frac{1}{\mathrm{N}(P)^s}\right)^{-1}$ и докажите, что ряд $\sum_A \frac{1}{\mathrm{N}(A)^s}$ сходится. 7. Пусть K – числовое поле, R – его кольцо целых, $\psi(a)$ – число идеалов R с нормой a, последовательность c_n определена как $c_n = \sum_{d\mid n} \mu(d)\psi(n/d)$. Докажите, что $\frac{\zeta_K(s)}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{c_n}{n^s}$. **SageMath:** ● Распределение простых чисел, распределение простых чисел в арифметических прогрессиях. Число классов поля, работа с базами данных NFDB и LMFDB.

5.4. Темы для самостоятельной работы по дисциплине

- Рациональные приближения и непрерывные дроби (после I.1)
- Линейные рекуррентные соотношения (после II.3)
- Алгоритм RSA (Textbook RSA) (после I.2)
- Частично гомоморфная схема Пэйе (после I.3)
- Криптосистема Гольдвассер-Микали (после I.4)
- Схема Эль-Гамаля (после II.1)
- Криптографическая схема NTRUEncrypt (после II.2)
- Линейный генератор псевдослучайных чисел (после I.3)
- Генератор псевдослучайных чисел Блюм-Блюма-Шуба (после I.3)
- Коды исправляющие ошибки, расстояние Хэмминга, оценка Плоткина (после II.1)
- Линейные коды (после II.1)
- Циклические коды, код как идеал кольца многочленов (после II.2)
- Весовая функция кода, двойственные коды, теорема Мак-Вильямс (после II.3)
- Квадратично-вычетные коды (после II.3)
- p-адические коды (после III.3)

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ (ФОС, ОЦЕНОЧНЫЕ И МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ) ДЛЯ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ).

6.1. Типовые контрольные задания или иные материалы для проведения текущего контроля успеваемости.

Вопросы к зачёту:

№	Вопрос	Раздел и тема дисциплины
1	Делимость в кольце целых чисел, алгоритм Евклида. Бесконечность числа простых чисел. Однозначное разложение целых чисел на простые множители	I.1
2	Мультипликативные функции, функции Эйлера и Мёбиуса. Формула обращения Мёбиуса	I.1
3	Неравенства Чебышева	I.1
4	Сравнения, полная и приведенная система вычетов. Число решений линейного сравнения. Теоремы Эйлера и Ферма	I.2
5	Китайская теорема об остатках	I.2
6	Однозначность разложения в кольце многочленов	I.2
7	Теорема Лагранжа о числе корней многочлена. Теорема Вильсона	I.3
8	Первообразные корни и структура группы единиц по модулю m	I.3
9	Степенные вычеты	I.3
10	Квадратичные вычеты, символ Лежандра и его свойства	I.4
11	Квадратичный закон взаимности	I.4
12	Сравнения по двойному модулю, существование неприводимых многочленов произвольной степени над конечным полем	II.1
13	Мультипликативная группа конечного поля	II.1
14	Автоморфизм Фробениуса, группа Галуа конечного поля	II.1
15	Круговое поле, группа корней из единицы	II.2
16	Круговой многочлен, разложение кругового многочлена на неприводимые множители над конечным полем	II.2
17	Норма и след, их свойства. Абсолютные и относительные норма и след	II.3
18	Характеры абелевых групп	II.3
19	Сумма Гаусса, значение её модуля	II.3
20	Теоремы Варинга и Шевалле	II.4
21	Теорема Виноградова-Пойя	II.4

22	Суммы Якоби и их свойства	II.4
23	Аффинное и проективное пространства над конечным полем	II.5
24	Соотношение Хассе-Дэвенпорта	II.5
25	Дзета функция Артина, критерий её рациональности	II.5
26	Построение кольца целых p-адических чисел	III.1
27	Делимость и единицы в кольце целых p-адических чисел, p-показатель и p-адическая метрика	III.1
28	Ряды и последовательности p-адических чисел, их сходимость	III.1
29	Метризованные поля, эквивалентность метрик пополнение по метрике	III.2
30	Теорема Островского	III.2
31	Неархимедовы метрики и их топологические свойства	III.2
32	Кольцо и идеал показателя. Локальные кольца	III.3
33	Лемма Гензеля	III.3
34	Делимость и разложение на множители в кольцах $\mathbb{Z}[i]$, $\mathbb{Z}[\omega]$	IV.1
35	Кубический и биквадртичный характеры. Высшие законы взаимности	IV.1
36	Числовые поля. Норма, след и дискриминант	IV.2
37	Дедекиндовы кольца, однозначность разложения на простые идеалы	IV.2
38	Квадратичное поле и его кольцо целых. Порядки в квадратичном поле	IV.3
39	Круговое поле и его кольцо целых. Круговой многочлен	IV.3
40	Характеры Дирихле. Ряды Дирихле и их свойства	V.1
41	Аналитическое продолжение рядов Дирихле	V.1
42	Теорема Дирихле	V.2
43	Дзета-фукнция Дедекинда	V.2

Примеры контрольных задач приведены в разделе 5.3.

7. РЕСУРСНОЕ ОБЕСПЕЧЕНИЕ:

7.1. Перечень основной и дополнительной литературы

Основная литература

[1] И.М. Виноградов, *Основы теории чисел*. Наука, 1981

[2] К. Айерленд, М. Роузен, *Классическое введение в современную теорию чисел*, МИР, 1987 (K. Ireland, M. Rosen, *A Classical Introduction to Modern Number Theory*. Springer, 1990)

[3] З.И. Боревич, И.Р. Шафаревич, *Теория чисел*. Наука, 1972

[4] Ж.-П. Серр, *Курс арифметики*. МИР, 1972 (J.-P. Serre, *Cours D'Arithmetique*, Presses Universitaire de France, 1970)

[5] С.А. Степанов, *Арифметика алгебраических кривых*. Наука, 1991

Дополнительная литература

[6] R. Lidl, H. Niederreiter, *Introduction to Finite Fields and their Applications*. Cambridge University Press, 1994

[7] F. Gouvêa, *p-adic Numbers: An Introduction*. Springer, 2020

[8] D.A. Marcus, *Number Fields*. Springer, 2018

[9] D.A. Cox, *Primes of the Form* $x^2 + ny^2$. Wiley, 2013

[10] G. Davidoff, P. Sarnak, A. Valette, *Elementary Number Theory, Group Theory, and Ramanujan Graphs*, Cambridge University Press, 2003

7.2. Перечень лицензионного программного обеспечения, в том числе отечественного производства

При реализации дисциплины может быть использовано следующее программное обеспечение:

- Операционная система Windows / Linux / MacOS
- Система компьютерной алгебры SageMath. Свободно-распространяемое ПО
- Язык программирования Python и среда разработки Jupiter Notebook. Свободно-распространяемое ПО
- Visual Studio Community Интегрированная среда разработки ПО. Свободно-распространяемое ПО
- Файловый архиватор 7z. Свободно-распространяемое ПО
- Браузеры Google Chrome, Mozilla Firefox. Свободно-распространяемое ПО
- Офисный пакет LibreOffice. Свободно-распространяемое ПО
- Программное обеспечение для создания и просмотра pdf-документов Adobe Reader
- Издательская система LaTeX

7.3. Перечень профессиональных баз данных и информационных справочных систем

1. http://www.edu.ru – портал Министерства образования и науки РФ
2. http://www.ict.edu.ru – система федеральных образовательных порталов «ИКТ в образовании»
3. http://www.openet.ru - Российский портал открытого образования
4. http://www.mon.gov.ru - Министерство образования и науки Российской Федерации
5. http://www.fasi.gov.ru - Федеральное агентство по науке и инновациям

7.4. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. Math-Net.Ru [Электронный ресурс] : общероссийский математический портал / Математический институт им. В. А. Стеклова РАН ; Российская академия наук, Отделение математических наук. - М. : [б. и.], 2010. - Загл. с титул. экрана. - Б. Ц. URL: http://www.mathnet.ru
2. Университетская библиотека Online [Электронный ресурс] : электронная библиотечная система / ООО "Директ-Медиа" . - М. : [б. и.], 2001. - Загл. с титул. экрана. - Б. ц. URL: www.biblioclub.ru
3. Универсальные базы данных EastView [Электронный ресурс] : информационный ресурс / EastViewInformationServices. - М. : [б. и.], 2012. - Загл. с титул. экрана. - Б. Ц. URL: www.ebiblioteka.ru
4. Научная электронная библиотека eLIBRARY.RU [Электронный ресурс] : информационный портал / ООО "РУНЭБ" ; Санкт-Петербургский государственный университет. - М. : [б. и.], 2005. - Загл. с титул. экрана. - Б. Ц. URL: www.eLibrary.ru
5. Sage Tutorial in Russian https://doc.sagemath.org/pdf/ru/tutorial/SageTutorial_ru.pdf
6. Number Fields Database (NFDB) https://hobbes.la.asu.edu/NFDB/
7. The L-functions and modular forms database (LMFDB) https://www.lmfdb.org

7.5. Описание материально-технического обеспечения.

Образовательная организация, ответственная за реализацию данной Программы, располагает соответствующей материально-технической базой, включая современную вычислительную технику, объединенную в локальную вычислительную сеть, имеющую выход в Интернет. Используются специализированные компьютерные классы, оснащенные современным оборудованием. Материальная база соответствует действующим санитарно-техническим нормам и обеспечивает проведение всех видов занятий (лекционных, практических, семинарских, лабораторных, дисциплинарной и междисциплинарной подготовки) и научно-исследовательской работы обучающихся, предусмотренных учебным планом.

8. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ОРГАНИЗАЦИИ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ

8.1. Формы и методы преподавания дисциплины

- Используемые формы и методы обучения: лекции и семинары, самостоятельная работа студентов.
- В процессе преподавания дисциплины преподаватель использует как классические формы и методы обучения (лекции и практические занятия), так и активные методы обучения.
- При проведении лекционных занятий преподаватель использует аудиовизуальные, компьютерные и мультимедийные средства обучения, а также демонстрационные и наглядно-иллюстрационные (в том числе раздаточные) материалы.
- Семинарские (практические) занятия по данной дисциплине проводятся с использованием компьютерного и мультимедийного оборудования, при

необходимости - с привлечением полезных Интернет-ресурсов и пакетов прикладных программ.

8.2. Методические рекомендации преподавателю

Перед началом изучения дисциплины преподаватель должен ознакомить студентов с видами учебной и самостоятельной работы, перечнем литературы и интернет-ресурсов, формами текущей и промежуточной аттестации, с критериями оценки качества знаний для итоговой оценки по дисциплине.

При проведении лекций, преподаватель:

- формулирует тему и цель занятия;
- излагает основные теоретические положения;
- сопровождает теоретические положения наглядными примерами (численные результаты и частные случаи);
- в конце занятия дает вопросы для самостоятельного изучения.

Во время выполнения заданий в учебной аудитории студент может консультироваться с преподавателем, определять наиболее эффективные методы решения поставленных задач. Если какая-то часть задания остается не выполненной, студент может продолжить её выполнение во время внеаудиторной самостоятельной работы.

Перед выполнением внеаудиторной самостоятельной работы преподаватель проводит инструктаж (консультацию) с определением цели задания, его содержания, сроков выполнения, основных требований к результатам работы, критериев оценки, форм контроля и перечня источников и литературы.

Для оценки полученных знаний и освоения учебного материала по каждому разделу и в целом по дисциплине преподаватель использует формы текущего, промежуточного и итогового контроля знаний обучающихся.

Для семинарских занятий

Подготовка к проведению занятий проводится регулярно. Организация преподавателем семинарских занятий должна удовлетворять следующим требования: количество занятий должно соответствовать учебному плану программы, содержание планов должно соответствовать программе, план занятий должен содержать перечень рассматриваемых вопросов.

Во время семинарских занятий используются словесные методы обучения, как беседа и дискуссия, что позволяет вовлекать в учебный процесс всех слушателей и стимулирует творческий потенциал обучающихся.

При подготовке семинарскому занятию преподавателю необходимо знать план его проведения, продумать формулировки и содержание учебных вопросов, выносимых на обсуждение.

В начале занятия преподаватель должен раскрыть теоретическую и практическую значимость темы занятия, определить порядок его проведения, время на обсуждение каждого учебного вопроса. В ходе занятия следует дать возможность выступить всем желающим и предложить выступить тем слушателям, которые проявляют пассивность.

Целесообразно, в ходе обсуждения учебных вопросов, задавать выступающим и аудитории дополнительные и уточняющие вопросы с целью выяснения их позиций по существу обсуждаемых проблем, а также поощрять выступление с места в виде кратких дополнений. На занятиях проводится отработка практических умений под контролем преподавателя

Для практических занятий

Подготовка преподавателя к проведению практического занятия начинается с изучения исходной документации и заканчивается оформлением плана проведения занятия.

На основе изучения исходной документации у преподавателя должно сложиться представление о целях и задачах практического занятия и о том объеме работ, который должен выполнить каждый обучающийся. Далее можно приступить к разработке содержания практического занятия. Для этого преподавателю (даже если он сам читает лекции по этому курсу) целесообразно вновь просмотреть содержание лекции с точки зрения предстоящего практического занятия. Необходимо выделить понятия, положения, закономерности, которые следует еще раз проиллюстрировать на конкретных задачах и упражнениях. Таким образом, производится отбор содержания, подлежащего усвоению.

Важнейшим элементом практического занятия является учебная задача (проблема), предлагаемая для решения. Преподаватель, подбирая примеры (задачи и логические задания) для практического занятия, должен представлять дидактическую цель: привитие каких навыков и умений применительно к каждой задаче установить, каких усилий от обучающихся она потребует, в чем должно проявиться творчество студентов при решении данной задачи.

Преподаватель должен проводить занятие так, чтобы на всем его протяжении студенты были заняты напряженной творческой работой, поисками правильных и точных решений, чтобы каждый получил возможность раскрыться, проявить свои способности. Поэтому при планировании занятия и разработке индивидуальных заданий преподавателю важно учитывать подготовку и интересы каждого студента. Педагог в этом случае выступает в роли консультанта, способного вовремя оказать необходимую помощь, не подавляя самостоятельности и инициативы студента.

8.3. Методические рекомендации студентам по организации самостоятельной работы.

Приступая к изучению новой учебной дисциплины, студенты должны ознакомиться с учебной программой, учебной, научной и методической литературой, имеющейся в библиотеке университета, встретиться с преподавателем, ведущим дисциплину, получить в библиотеке рекомендованные учебники и учебно-методические пособия, осуществить запись на соответствующий курс в среде электронного обучения университета.

Глубина усвоения дисциплины зависит от активной и систематической работы студента на лекциях и практических занятиях, а также в ходе самостоятельной работы, по изучению рекомендованной литературы.

На лекциях важно сосредоточить внимание на ее содержании. Это поможет лучше воспринимать учебный материал и уяснить взаимосвязь проблем по всей дисциплине. Основное содержание лекции целесообразнее записывать в тетради в виде ключевых фраз, понятий, тезисов, обобщений, схем, опорных выводов. Необходимо обращать внимание на термины, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации. Желательно оставлять в конспектах поля, на которых делать пометки из рекомендованной литературы, дополняющей материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений. С целью уяснения теоретических положений, разрешения спорных ситуаций необходимо задавать преподавателю уточняющие вопросы. Для закрепления содержания лекции в памяти, необходимо во время самостоятельной работы внимательно прочесть свой конспект и дополнить его записями из учебников и рекомендованной литературы.

Конспектирование читаемых лекций и их последующая доработка способствует более глубокому усвоению знаний, и поэтому являются важной формой учебной деятельности студентов.

Методические указания для обучающихся по подготовке к семинарским занятиям

Для того чтобы семинарские занятия приносили максимальную пользу, необходимо помнить, что упражнение и решение задач проводятся по вычитанному на лекциях материалу и связаны, как правило, с детальным разбором отдельных вопросов лекционного курса. Следует подчеркнуть, что только после усвоения лекционного материала с определенной точки зрения (а именно с той, с которой он излагается на лекциях) он будет закрепляться на семинарских занятиях как в результате обсуждения и анализа лекционного материала, так и с помощью решения проблемных ситуаций, задач.

При этих условиях студент не только хорошо усвоит материал, но и научится применять его на практике, а также получит дополнительный стимул (и это очень важно) для активной проработки лекции.

При самостоятельном решении задач нужно обосновывать каждый этап решения, исходя из теоретических положений курса. Если студент видит несколько путей решения проблемы (задачи), то нужно сравнить их и выбрать самый рациональный. Полезно до начала вычислений составить краткий план решения проблемы (задачи). Решение проблемных задач или примеров следует излагать подробно, вычисления располагать в строгом порядке, отделяя вспомогательные вычисления от основных. Решения при необходимости нужно сопровождать комментариями, схемами, чертежами и рисунками.

Следует помнить, что решение каждой учебной задачи должно доводиться до окончательного логического ответа, которого требует условие, и по возможности с выводом. Полученный ответ следует проверить способами, вытекающими из существа данной задачи. Полезно также (если возможно) решать несколькими способами и сравнить полученные результаты. Решение задач данного типа нужно продолжать до приобретения твердых навыков в их решении.

При подготовке к семинарским занятиям следует использовать основную литературу из представленного списка, а также руководствоваться приведенными указаниями и рекомендациями. Для наиболее глубокого освоения дисциплины рекомендуется изучать литературу, обозначенную как «дополнительная» в представленном списке.

Методические указания для обучающихся по подготовке к практическим занятиям

Целью практических занятий по данной дисциплине является закрепление теоретических знаний, полученных при изучении дисциплины.

При подготовке к практическому занятию целесообразно выполнить следующие рекомендации: изучить основную литературу; ознакомиться с дополнительной литературой, новыми публикациями в периодических изданиях: журналах, газетах и т. д.; при необходимости доработать конспект лекций. При этом учесть рекомендации преподавателя и требования учебной программы.

При выполнении практических занятий основным методом обучения является самостоятельная работа студента под управлением преподавателя. На них пополняются теоретические знания студентов, их умение творчески мыслить, анализировать, обобщать изученный материал, проверяется отношение студентов к будущей профессиональной деятельности.

Оценка выполненной работы осуществляется преподавателем комплексно: по результатам выполнения заданий, устному сообщению и оформлению работы. После подведения итогов занятия студент обязан устранить недостатки, отмеченные преподавателем при оценке его работы.

Методические указания для самостоятельной работы обучающихся

Прочное усвоение и долговременное закрепление учебного материала невозможно без продуманной самостоятельной работы. Такая работа требует от студента значительных усилий, творчества и высокой организованности. В ходе самостоятельной работы студенты выполняют следующие задачи: дорабатывают лекции, изучают рекомендованную литературу, готовятся к практическим занятиям, к коллоквиуму, контрольным работам по отдельным темам дисциплины. При этом эффективность учебной деятельности студента во многом зависит от того, как он распорядился выделенным для самостоятельной работы бюджетом времени.

Результатом самостоятельной работы является прочное усвоение материалов по предмету согласно программы дисциплины. В итоге этой работы формируются профессиональные умения и компетенции, развивается творческий подход к решению возникших в ходе учебной деятельности проблемных задач, появляется самостоятельности мышления.