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/
«____»_____ 2025 г.

Рабочая программа дисциплины (модуля)

Наименование дисциплины (модуля):
Основы алгебраической теории чисел

Уровень высшего образования:
магистратура

Направление подготовки / специальность:
01.04.02 «Прикладная математика и информатика»

Направленность (профиль) ОПОП:
дисциплина относится к вариативной части программы
«Информационная безопасность компьютерных систем»

Форма обучения:
очная

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

Москва 2025

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».

Содержание

1 Место дисциплины (модуля) в структуре ОПОП ВО

Настоящая дисциплина включена в учебный план по направлению 01.04.02 «Прикладная математика и информатика», профиль «Информационная безопасность компьютерных систем» и входит в базовую часть программы. Дисциплина является кафедральным (вариативным) курсом и изучается по выбору студента. Дисциплина рассчитана на студентов, знакомых с основными понятиями и результатами линейной алгебры, действительного 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. Даётся теоретический материал, необходимый для последующего изучения прикладных курсов по криптографии и теории кодирования, а также продвинутых курсов по современной теории чисел, алгебраической геометрии и алгебраической топологии. 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.

3 Результаты обучения по дисциплине (модулю)

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

Содержание и код компетенции

- **ОПК-1.** Способность формулировать и решать актуальные задачи в области фундаментальной и прикладной математики.
- **ОПК-4.** Способность комбинировать и адаптировать современные информационно-коммуникационные 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 её приложений, используя современные информационно-коммуникационные технологии.

Индикатор (показатель) достижения компетенции

- **СПК-ВТЧП-1М.1.** Владение основными понятиями и методами элементарной теории чисел
- **СПК-ВТЧП-1М.2.** Владение основными понятиями и результатами связанными с 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

Планируемые результаты обучения по дисциплине, сопряженные с индикаторами достижения компетенций

- **Знать**
  - Основные понятия, определения и результаты элементарной теории чисел
  - Основные понятия, определения и результаты теории конечных полей
  - 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 136 академических часов, в том числе 68 академических часов, отведенных на контактную работу обучающихся с преподавателем, 68 академических часов на самостоятельную работу обучающихся.

5 Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведённого на них количества академических часов и видов 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)

	Номинальные трудозатраты обучающегося, академические часы				
Наименование разделов и тем дисциплины (модуля), Форма промежуточной аттестации по дисциплине (модулю)	Контактная работа, занятия лекционного типа	Контактная работа, занятия семинарского типа	Самостоятельная работа обучающегося	**Всего академических часов**	**Форма текущего контроля успеваемости* (наименование)**
Раздел 1. Элементарная теория чисел					
Тема 1. Простые числа	2	2	4	8	
Тема 2. Сравнения	2	2	4	8	
Тема 3. Первообразные корни	2	2	4	8	
Тема 4. Квадратичные вычеты	2	2	4	8	
Раздел 2. Конечные поля и тригонометрические суммы					
Тема 5. Конечные поля. Расширения полей	2	2	4	8	
Тема 6. Группа автоморфизмов. Норма и след	2	2	4	8	
Тема 7. Корни из единицы. Круговой многочлен	2	2	4	8	
Тема 8. Характеры. Суммы Гаусса	2	2	4	8	

Тема 9. Тригонометрические суммы. Уравнения над конечными полями	2	2	4	8	
Тема 10. Дзета-функция Артина	2	2	4	8	
Раздел 3. p-адические числа					
Тема 11. p-адические числа: элементарное определение и свойства	2	2	4	8	
Тема 12. Аксиоматическое определение поля p-адических чисел, метризованные поля	2	2	4	8	
Тема 13. Лемма Гензеля, принцип Хассе	2	2	4	8	
Раздел 4. Числовые поля					
Тема 14. Кольцо целых гауссовых чисел	2	2	4	8	
Тема 15. Арифметика колец целых алгебраических чисел	2	2	4	8	
Тема 16. Квадратичное поле и круговое поле	2	2	4	8	
Итоговая аттестация					**зачет**
Итого, академические часы	**32**	**32**	**64**	**128**	

5.2 Содержание разделов (тем) дисциплины

Курс состоит из четырёх 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.

р-адический анализ является важным инструментом современной криптографии, а область р-адических динамических систем имеет много других приложений. В первой лекции раздела дается прямое построение кольца целых р-адических чисел, рассматриваются его основные арифметические свойства, изучаются вопросы сходимости р-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 р-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.

Наименование разделов (тем) дисциплины	**Содержание разделов (тем) дисциплин**
Раздел 1. Элементарная теория чисел	*Источники: [Вин], главы 1-5; [IR]*
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 2. Конечные поля и тригонометрические суммы	*Источники: [Степ], главы I-II; [IR], главы 7-8; [Serre], глава I; [ЛН], главы 2,5; [БШ], §§I.1-I.2, АД.2-АД.3*
Тема 5. Конечные поля. Расширения полей	Конечное поле $\mathbb{F}_q$ как фактор-кольцо кольца многочленов $\mathbb{F}_p[x]$. Количество неприводимых многочленов над $\mathbb{F}_p$. Цикличность мультипликативной группы $\mathbb{F}_q^*$. Конечные расширения полей, свойства расширения $\mathbb{F}_q/\mathbb{F}_p$.
Тема 6. Группа автоморфизмов. Норма и след	Подполя конечных полей. Автоморфизм Фробениуса, цикличность группы Галуа конечного поля. Соответствие Галуа для башни конечных полей. Норма и след для произвольных конечных расширений полей. Дискриминант базиса расширения. Свойства нормы и следа в случае конечных полей.
Тема 7. 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 8. Характеры. Суммы Гаусса	Характеры конечных абелевых групп. Двойственная группа. Свойства ортогональности. Аддитивные и мультипликативные характеры конечного поля. Суммы Гаусса, обобщённые суммы Гаусса. Соотношение Хассе-Дэвенпорта.

Тема 9. Тригонометрические суммы. Уравнения над конечными полями	Связь тригонометрических сумм с числом решений уравнений в конечных полях. Суммы Якоби и их приложения для числа решений уравнений. Теоремы Варинга и Шевалле. Суммы характеров. Неполные суммы характеров. Теорема Виноградова-Пойя.
Тема 10. Дзета функция Артина	Элементы алгебраической геометрии над конечным полем: аффинное и проективное пространства, уравнения как гиперповерхности. Дзета функция Артина, критерий её рациональности. Дзета функция гиперповерхности заданной формой $a_0x_0^m + \cdots + a_nx_n^m$ и её рациональность.
Раздел 3. p-адические числа	*Источники: [БШ], глава I; [Serre], глава II; [Gouv], главы 1-4]*
Тема 11. 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 12. 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 13. Лемма Гензеля, принцип Хассе	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 4. Числовые поля	*Источники: [IR], главы 9,12-13; [БШ], глава III; [Marc], главы 2-5; [Cox], §I.4, §II.7; [DSV], глава 2*
Тема 14. Кольцо целых гауссовых чисел	Евклидовы кольца, кольца главных идеалов. Однозначность разложения на множители в кольцах главных идеалов. Кольцо гауссовых чисел $\mathbb{Z}[i]$ и кольцо чисел Эйзенштейна $\mathbb{Z}[\omega]$. Число представлений целого в виде суммы двух квадратов. Суммы четырёх квадратов, связь с алгеброй кватернионов.

Тема 15. Арифметика колец целых алгебраических чисел	Числовые поля, кольца алгебраических целых чисел. Нётеровы кольца. Однозначность разложения в кольце алгебраических целых чисел. Элементы теории Галуа числовых полей. Применение теории Галуа к разложению на простые идеалы в башнях полей и колец.
Тема 16. 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.

5.3 Примеры задач для семинаров и самостоятельной работы

Тема 1. Простые числа

Упражнения и задачи

1. Докажите свойства делимости:
   - $a|a$, $a \neq 0$;
   - $a|b, b|a \implies a = \pm b$;
   - $a|b, b|c \implies a|c$;
   - $a|b, a|c \implies a|b \pm c$.

2. Алгоритм Евклида: Пусть $a, b \in \mathbb{Z} \setminus \{0\}, a > b$, определим последовательность $b > r_1 > r_2 > \cdots > r_n$ следующим образом: $a = bq_0 + r_1$, $b = r_1q_1 + r_2$, $r_1 = r_2q_2 + r_3, \ldots r_n = r_{n-1}q_{n-1} + r_n$. Докажите, что $\exists n : r_{n-1} = r_nq_n$ и $r_n = (a, b)$. (Сначала докажите , что $(a, b) = (b, r_1)$).

3. Докажите, что $\sqrt{2}$ — иррациональное число, т.е. что не $\exists$ рационального $r = a/b$ $(a, b \in \mathbb{Z})$ такого, что $r^2 = 2$.

4. Пусть $\alpha \in \mathbb{R}$, $b \in \mathbb{Z}_+$, докажите, что $\left[\dfrac{[\alpha]}{b}\right] = \dfrac{\alpha}{b}$.

5. Пусть $(a, b) = 1$, докажите, что $(a + b, a - b) = 1$ или 2.

6. Пусть $a, b, c \in \mathbb{Z}$, докажите что уравнение $ax + by = c$ разрешимо в целых числах $\iff d = (a, b)|c$. Докажите также, что если x_0, y_0 — решение этого уравнения, то все решения имеют вид $x = x_0 + t\dfrac{b}{d}$, $y = y_0 - t\dfrac{b}{d}$, где $t \in \mathbb{Z}$.

7. Докажите следующие свойства:
   - $\nu_p([a, b]) = \max(\nu_p(a), \nu_p(b))$;

- $\nu_p(a+b) \geqslant \min(\nu_p(a), \nu_p(b))$, причем $\nu_p(a+b) = \min(\nu_p(a), \nu_p(b))$, если $\nu_p(a) \neq \nu_p(b)$;
- $(a,b)[a,b] = ab$;
- $(a+b, [a,b]) = (a,b)$.

8. Докажите, что $\nu_p(n!) = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \dots$

9. Докажите, что существует бесконечно много простых вида $4k-1$, $k \in \mathbb{Z}$.

10. Пусть $a, b, c, d \in \mathbb{Z}$, $(a,b) = 1$, $(c,d) = 1$. Докажите, что если $\frac{a}{b} + \frac{c}{d} \in \mathbb{Z}$, то $b = \pm d$.

11. Пусть $n \in \mathbb{Z}$, $n > 2$ Докажите, что числа
$$\frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{n};\ \frac{1}{3} + \frac{1}{5} + \dots + \frac{1}{2n+1}$$
не являются целыми.

12. Пусть $f(n)$ — мультипликативная функция. Докажите, что функции
$$g(n) = \sum_{d|n} f(d),\ h(n) = \sum_{d|n} \mu(\frac{n}{d}) f(d)$$
также мультипликативны.

13. Докажите, что $\forall n \in \mathbb{Z}$
$$\sum_{d|n} \mu(\frac{n}{d})\nu(d) = 1,\ \sum_{d|n} \mu(\frac{n}{d})\sigma(d) = n.$$

14. Докажите, что $\forall m, n \in \mathbb{Z}$
    - $\varphi(n)\varphi(m) = \varphi((n,m))\varphi([n,m])$;
    - $\varphi(mn)\varphi((m,n)) = (m,n)\varphi(m)\varphi(n)$.

15. Пусть $P, Q \in \mathbb{Z}_+$ — нечетные, $(P,Q) = 1$. Докажите, что
$$\sum_{0<x<\frac{Q}{2}} \left[\frac{P}{Q}x\right] + \sum_{0<y<\frac{P}{2}} \left[\frac{Q}{P}y\right] = \frac{P-1}{2}\frac{Q-1}{2}.$$
(Используйте подсчет целых точек в некоторой ограниченной области на плоскости).

SageMath

- Исследуйте основные теоретико-числовые функции в SageMath:
  - НОД, НОК: `gcd(), xgcd(), lcm()`;
  - разложение на множители: `factor(), valuation()`;
  - простые числа: `is_prime(), next_prime(), previous_prime()`;
  - делители: `divisors(), prime_divisors()` ;
  - функции Эйлера и Мёбиуса, число и сумма делителей: `euler_phi(), moebius(), sigma()`;
  - число простых чисел: `prime_pi()` (постройте график этой функции).

Тема 2. Сравнения

Упражнения и задачи

1. Докажите, что $\equiv \pmod m$ задаёт отношение эквивалентности в кольце $\mathbb{Z}$, то есть, 1) $a \equiv a\,(m)$; 2) $a \equiv b\,(m) \Rightarrow b \equiv a\,(m)$; 3) $a \equiv b\,(m),\ b \equiv c\,(m) \Rightarrow a \equiv c\,(m)$.

2. Докажите утверждения про классы вычетов:

   - $\bar{a} = \bar{b} \Leftrightarrow a \equiv b\ (m)$;
   - $\bar{a} \neq \bar{b} \Leftrightarrow \bar{a} \cap \bar{b} = \varnothing$;
   - $|\{\bar{a} : a \in \mathbb{Z}\}| = m$.

3. Докажите, что операции $\bar{a} + \bar{b}$, $\bar{a} \cdot \bar{b}$ на множестве классов вычетов корректно определены, то есть не зависят от выбора представителей классов $\bar{a}$ и $\bar{b}$.

4. Докажите, что множество $F[x]$ многочленов с коэффициентами из поля F является кольцом.

5. Докажите, что $\forall f \in F[x]$, $\deg f \geqslant 1$, f раскладывается в произведение неприводимых многочленов.

6. Докажите, что в кольце $F[x]$ возможно деление с остатком, т.е. $\forall f, g \in F[x]$, $g \neq 0$, $\exists h, r \in F[x] : f = hg + r$, где либо $\deg r < \deg g$, либо $r = 0$.

7. Докажите следующие утверждения про делимость в кольце многочленов:

   - $f, g \in F[x]$ — взаимно простые (т.е. $(f, g) = (1)$), $f|gh \Rightarrow f|h$;
   - $p \in F[x]$ — неприводимый, $p|fg \Rightarrow p|f$ или $p|g$.

8. Докажите, что в кольце многочленов $F[x]$ имеет место однозначнось разложения на неприводимые множители.

9. Используя сравнимость $\bmod n$ докажите, что уравнения $3x^2 + 2 = y^2$ и $7x^3 + 2 = y^3$ не разрешимы в целых числах.

10. Пусть p, q — различные нечетные простые такие что $p - 1|q - 1$, докажите, что если $(n, pq) = 1$ то $n^{q-1} \equiv 1(pq)$.

11. Пусть a, b, c — решение диофантова уравнения $a^2 + b^2 = c^2$, $a, b, c \in \mathbb{Z}$, $(a, b) = (b, c) = (c, a) = 1$. Докажите, что существуют целые числа u, v такие, что $c - b = 2u^2$, $c + b = 2v^2$, $(u, v) = 1$, и, как следствие, $a = 2uv$, $b = v^2 - u^2$, $c = v^2 + u^2$.

12. Пусть m, a, b — целые, $m > 1$, $(a, m) = 1$. Докажите, что

    - $\sum\limits_{x \pmod m} \left\{\dfrac{ax + b}{m}\right\} = \dfrac{1}{2}(m - 1)$;
    - $\sum\limits_{\substack{x \pmod m \\ (x,m)=1}} \left\{\dfrac{ax}{m}\right\} = \dfrac{1}{2}\varphi(m)$.

SageMath

- Исследуйте основные классы и функции SageMath релевантные материалу лекции:
  - Кольцо вычетов и модулярная арифметика: `Integers()`;
  - Китайская теорема об остатках `crt()`;
  - Кольцо многочленов: `PolynomialRing()`;
  - Неприводимость многочлена: `is_irreducible()`;
  - Разложение многочлена на множители: `factor()`;
  - Корни многочлена: `roots()`;
  - Рассмотрите примеры поведения разложения многочлена на множители над $\mathbb{Z}, \mathbb{Q}$ и различными кольцами вычетов $\mathbb{Z}/N\mathbb{Z}$.

Темы для самостоятельного изучения

- Быстрое возведение в степень в $\mathbb{Z}/n\mathbb{Z}$, [Stein-ent], §2.3.
- Проверка на простоту, [Stein-ent], §2.4.

Тема 3. Первообразные корни

Упражнения и задачи

1. Путь p — простое, докажите, что $p|\binom{n}{k}$ для $1 \leqslant k < p$.
2. Путь $p > 2$ — простое, $l \geqslant 2$. Докажите, что $\forall a \in \mathbb{Z}\ (1+ap)^{p^{l-2}} \equiv 1 + ap^{l-1}\ (p^l)$.
3. Пусть $p > 2$ — простое, g — первообразный корень $\bmod p^n$. Докажите, что тогда g — первообразный корень $\bmod p$.
4. Пусть p — простое, $p \equiv 1 (\bmod 4)$. Докажите что g — первообразный корень $(\bmod p) \Leftrightarrow -g$ — первообразный корень $(\bmod p)$.
5. Пусть p — простое, $p \equiv 3 (\bmod 4)$. Докажите что g — первообразный корень $(\bmod p) \Leftrightarrow -g$ имеет порядок $(p-1)/2$.
6. Докажите, что 3 — первообразный корень простого числа вида $p = 2^n + 1$.
7. Пусть $p > 2$ — простое. Докажите, что g — первообразный корень $\bmod p \Leftrightarrow a^{(p-1)/q} \not\equiv 1(p)$ для всех простых делителей $q \mid p-1$.
8. Докажите, что $\prod\limits_g{}' g \equiv (-1)^{\varphi(p-1)}\ (p)$, где $\prod'$ — произведение по всем $0 \leqslant g \leqslant p-1$, g — первообразный корень $\bmod p$.
9. Пусть g — первообразный корень $\bmod p$, $d|(p-1)$. Докажите, что $g^{(p-1)/d}$ имеет порядок d, а также что a является d-ой степенью $\Leftrightarrow a \equiv g^{kd}(p)$ для некоторого k.
10. Пусть G — конечная циклическая группа порядка n, g — образующая G. Докажите, что все образующие имеют вид g^k, $(k,n) = 1$.
11. 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

- Исследуйте основные классы и функции SageMath релевантные материалу лекции:
  - Первообразные корни: `primitive_root(), is_primitive_root()`;
  - Образующие группы единиц: `unit_gens()`;
  - Порядок элемента в кольце вычетов: `multiplicative_order()`;
  - Индекс и дискретный логарифм в кольце вычетов: `log()`;
  - Абелевы группы `AbelianGroup()`, образующие и порядки `gens(), gens_orders()`.

- Пусть a — наименьшее положительное число являющееся первообразным корнем $\bmod p$. Постройте частотную таблицу для a, что можно заметить?

- Пусть $a \neq -1$ и не является полным квадратом. Постройте примеры последовательностей простых, для которых a является первообразным корнем (согласно гипотезе Артина таких простых бесконечно много, также можно оценить плотность их распределения).

Темы для самостоятельного изучения

- Структура группы единиц $U(\mathbb{Z}/2^l\mathbb{Z})$ ([IR, глава 4], [Вин, глава 6]).

- Критерии разрешимости сравнения $x^n \equiv a (\bmod n)$ ([IR, глава 4]).

- Основы криптографии с открытым ключем: протокол Диффи–Хеллмана и RSA, [Stein-ent], глава 3.

Тема 4. Квадратичные вычеты

Упражнения и задачи

1. Докажите, что существует бесконечно много простых $p \equiv 1\ (4)$ и $p \equiv 3\ (4)$.

2. Докажите, что $\left\lceil \frac{p-1}{4} \right\rceil$ четно $\Leftrightarrow p = 8k \pm 1$.

3. Докажите свойства символа Якоби:
   - $a \equiv b\ (P) \Rightarrow \left(\frac{a}{P}\right) = \left(\frac{b}{P}\right)$;
   - $\left(\frac{ab}{P}\right) = \left(\frac{a}{P}\right)\left(\frac{b}{P}\right)$;
   - $\left(\frac{a}{PQ}\right) = \left(\frac{a}{P}\right)\left(\frac{a}{Q}\right)$.

4. Пусть α — иррациональное число. Докажите, что последовательность $(\{n\alpha\})_{n=1}^{\infty}$ равномерно распределена $\bmod 1$.

5. Пусть p — простое, $(a, p) = 1$. Докажите, что число решений сравнения $ax^2 + bx + c \equiv 0\ (\bmod\ p)$ равно $1 + \left(\frac{b^2-4ac}{p}\right)$.

6. Докажите, что если $(a, p) = 1$ то $\sum_{x \bmod p} \left(\frac{ax+b}{p}\right) = 0$.

7. 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 $p|a$. Выразите число решений этого сравнения через сумму с символом Лежандра. Используя эти выражения, найдите значение для суммы $\sum_{y \bmod p} \left(\frac{y^2+a}{p}\right)$.

8. Докажите, что если $(a,p)=1$ то $\sum_{x \bmod p} \left(\frac{x(x+a)}{p}\right) = -1$.

9. Пусть $r_1, \ldots, r_{(p-1)/2}$ — квадратичные вычеты в промежутке $[1;p]$. Докажите, что их произведение $\equiv 1\ (p)$, если $p \equiv 3\ (4)$, и $\equiv -1\ (p)$, если $p \equiv 1\ (4)$.

10. Пусть $p \equiv 1\ (4)$ — простое, $(a,p)=1$, $S(a) = \sum_{x \bmod p} \left(\frac{x(x^2+a)}{p}\right)$. Докажите, что
    - $S(a) \equiv 0\ (2)$;
    - $S(at^2) = \left(\frac{t}{p}\right) S(a)$;
    - если r, n — такие, что $\left(\frac{r}{p}\right) = 1$, $\left(\frac{n}{p}\right) = -1$, то $p = \left(\frac{1}{2}S(r)\right)^2 + \left(\frac{1}{2}S(n)\right)^2$.

11. Пусть $f(x) \in \mathbb{Z}[x]$. Будем говорить, что простое p делит $f(x)$, если $\exists n \in \mathbb{Z}$ такое, что $p|f(n)$. Опишите простые делители многочленов x^2+1 и x^2-2. Докажите, что если p делит $x^4 - x^2 + 1$, то $p \equiv 1\ (12)$.

12. Пусть $D > 0$ — нечетное и свободное от квадратов. Докажите, что $\exists b \in \mathbb{Z}$, $(b,D)=1$ такое, что $\left(\frac{b}{D}\right) = -1$. Докажите также, что $\sum{}' \left(\frac{a}{D}\right) = 0$, где суммирование берется по приведенной системе вычетов $\bmod D$.

13. Пусть p — нечетное простое. Докажите, что
$$\left(\frac{2}{p}\right) = \prod_{j=1}^{(p-1)/2} 2\cos\left(\frac{2\pi j}{p}\right),$$
а также, что если $p > 3$ то
$$\left(\frac{3}{p}\right) = \prod_{j=1}^{(p-1)/2} \left(3 - 4\sin^2\left(\frac{2\pi j}{p}\right)\right).$$

SageMath

- Исследуйте основные функции SageMath связанные с вычислением квадратичных вычетов и символов Лежандра и Якоби:
  - Квадратичные вычеты: `quadratic_residues()`;
  - Символы: `legendre_symbol(), jacobi()`.

- Пусть $r(p)$ — наименьший квадратичный вычет $\bmod p$, $n(p)$ — наименьший квадратичный невычет $\bmod p$, $d(p)$ — максимальное расстояние между соседними квадратичными невычетами $\bmod p$. Постройте частотные таблицы для $r(p), n(p), d(p)$. Что можно заметить?
  (Согласно гипотезам Виноградова, $\forall \varepsilon > 0$ $\frac{d(p)}{p^\varepsilon} \to 0$, $\frac{n(p)}{p^\varepsilon} \to 0$, $\frac{r(p)}{p^\varepsilon} \to 0$ при $p \to \infty$.)

- Проведите численные эксперименты относительно равномерного распределения последовательностей, которые упоминались в лекции:

– $(\{n\alpha\})_{n=1}^{\infty}$, α — иррациональное;
– $(\{p\alpha\})_{p=1}^{\infty}$, α — иррациональное, p пробегает все простые;
– $(\{\frac{x_p}{p}\})_{p=1}^{\infty}$, x_p — решение сравнения $x^2 \equiv a\ (p)$, p пробегает все простые.

Темы для самостоятельного изучения

- Когда простое q является квадратичным вычетом по модулю простого p? (Приложение квадратичного закона взаимности, [IR, §5.2, теорема 2]).
- Существует бесконечно много простых таких, что $\left(\frac{a}{p}\right) = -1$, где a — целое, отличное от квадрата. ([IR, §5.2, теорема 3]).
- Критерий разрешимости сравнения $x^2 \equiv a\ (m)$ для произвольного m. ([IR, §5.1, предложение 5.1.1], [Вин, §V.4]).

Тема 5. Конечные поля. Расширения полей

Упражнения и задачи

1. Завершите доказательство леммы: пусть k — поле характеристики p, тогда $\forall \alpha, \beta \in k\ \forall d \in \mathbb{Z}_+\ (\alpha+\beta)^{p^d} = \alpha^{p^d} + \beta^{p^d}$.
2. Докажите, что многочлен x^2+x+1 неприводим над $\mathbb{F}_2$ (т.е. $\mathbb{F}_2[x]/(x^2+x+1)$ является полем). Выпишите таблицы операций сложения и умножения элементов в этом поле, а также обратные элементы.
3. Найдите все неприводимые многочлены степени 4 над полем $\mathbb{F}_2$.
4. Пусть L/K, M/L — конечные расширения (произвольных) полей. Докажите, что расширение M/K также конечно и $[M:K] = [K:L][L:K]$.
5. Докажите, что если L/K — конечное расширение, то оно является алгебраическим.
6. Пусть $q = p^n$, $\mathbb{F}_{q^m}/\mathbb{F}_q$ — расширение. Докажите, что если $f \in \mathbb{F}_q$ — неприводимый, то $\mathbb{F}_{q^m}$ — поле разложения f.
7. Пусть p, q — различные простые. Чему равно число неприводимых многочленов степени q в $\mathbb{F}_p[x]$?
8. Докажите следующие оценки для числа неприводимых многочленов степени n над $\mathbb{F}_p$:
$$\tfrac{1}{n}p^n - \tfrac{p}{n(p-1)}(p^{\frac{n}{2}} - 1) \leqslant \nu(n) \leqslant \tfrac{1}{n}(p^n - p).$$
9. Пусть $\sigma_j(f) = \sum'_{g|f}(Ng)^j$, где суммирование берется по неприводимым унитарным делителям g (для $f \in \mathbb{F}_q[x]$ степени $\deg f = n$ $Nf = q^n$). Докажите, что
   - $\sum\limits_f \dfrac{\sigma_0(f)}{(Nf)^s} = \dfrac{1}{(1-q^{1-s})^2}$;
   - $\sum\limits_f \dfrac{\sigma_1(f)}{(Nf)^s} = \dfrac{1}{(1-q^{1-s})(1-q^{2-s})}$.

10. Пусть $\alpha \in \mathbb{F}_q^*$. Докажите, что $x^n = \alpha$ разрешимо $\Leftrightarrow \alpha^{(q-1)/d=1}$, где $d = (n, q-1)$, причем если разрешимо, то d решений.

11. Как выглядит подгруппа всех квадратов в $\mathbb{F}_{2^n}$?

12. Пусть $n|q-1$, докажите, что $G = \{\alpha \in \mathbb{F}_q^* : x^n = \alpha$ — разрешимо$\}$ — подгруппа в $\mathbb{F}_q^*$, $|G| = \frac{q-1}{n}$.

13. Пусть $n|q-1$, $F = \mathbb{F}_q$, K/F — расширение конечных полей, $[K : F] = n$. Докажите, что $\forall \alpha \in F^*$ уравнение $x^n = \alpha$ имеет n решений в K.

14. Пусть K/F — расширение конечных полей, $\operatorname{char} F \neq 2$, $[K : F] = 3$. Докажите, что если α не является квадратом в F, то α не является квадратом и в K.

15. Пусть $F = \mathbb{F}_q$, K/F — расширение конечных полей, $\alpha \in \mathbb{F}_q$, $n|q-1$ и $x^n = \alpha$ не разрешимо в $\mathbb{F}_q$. Тогда $x^n = \alpha$ не разрешимо в K, если $(n, [K : F]) = 1$.

16. Пусть $F = \mathbb{F}_q$, K/F — расширение конечных полей, $[K : F] = 2$. Докажите, что $\forall \beta \in K$ $\beta^{1+q} \in F$. Более того, $\forall \alpha \in F$ $\exists \beta \in K$: $\alpha = \beta^{1+q}$.

SageMath

- Исследуйте основные функции SageMath связанные с заданием и свойствами конечных полей
  - Определение конечного поля: `FiniteField(), GF()`;
  - Неприводимый многочлен задающий конечное поле: `polynomial()`, опция `modulus` в `FiniteField()` для явного задания неприводимого многочлена модели конечного поля;
  - Решение уравнения $x^n = \alpha$: `nth_root()`;
  - Поле разложения: `splitting_field()`;
  - Расширение полей: `extension()`.

Темы для самостоятельного изучения

- Поле $\mathbb{F}_q$, $q = p^n$, однозначно определено в $\bar{\mathbb{F}}_p$ как поле разложения многочлена $z^q - z$. Всякое конечное поле изоморфно одному и только одному $\mathbb{F}_q$. ([Степ], [LN])

Тема 6. Группа автоморфизмов. Норма и след

Упражнения и задачи

1. Докажите, что
   - для $a \in \mathbb{Z}$ $a^l - 1 | a^m - 1 \Leftrightarrow l|m$
   - в $\mathbb{F}_q[x]$ $x^l - 1 | x^m - 1 \Leftrightarrow l|m$

2. Завершите доказательсво теоремы о цикличности $\operatorname{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$: покажите, что $|\operatorname{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)| \leqslant n$.

3. Докажите, что характеристический многочлен $g_\alpha(x)$ и определитель $\det A_\alpha$ не зависят от выбора базиса расширения L/K.

4. Докажите следующие свойства нормы и следа:

(a) $\mathrm{N}_{L/K}(a) = a^n$, $\mathrm{Tr}_{L/K}(a) = na$, $a \in K$;
(b) $\mathrm{N}_{L/K}(\alpha\beta) = \mathrm{N}_{L/K}(\alpha)\,\mathrm{N}_{L/K}(\beta)$, $\alpha, \beta \in L$;
(c) $\mathrm{N}_{L/K}(a\alpha) = a^n\,\mathrm{N}_{L/K}(\alpha)$, $\mathrm{Tr}_{L/K}(a\alpha) = a\,\mathrm{Tr}_{L/K}(\alpha)$, $a \in K$, $\alpha \in L$.

5. Пусть L/K — расширение, $\alpha \in L$, $g_\alpha(x)$ — характеристический многочлен α, M/K — расширение, в котором $g_\alpha(x)$ полностью раскладывается на линейные множители: $g_\alpha(x) = (x - \alpha_1)\dots(x - \alpha_n)$. Докажите, что:
$$\mathrm{N}_{L/K}(\alpha) = \alpha_1 \dots \alpha_n,\ \mathrm{Tr}_{L/K}(\alpha) = \alpha_1 + \dots + \alpha_n.$$

6. Пусть L/K, M/L — конечные расширения, $\gamma \in M$. Докажите, что $\mathrm{N}_{M/K}(\gamma) = \mathrm{N}_{L/K}(\mathrm{N}_{M/L}(\gamma))$, $\mathrm{Tr}_{M/K}(\gamma) = \mathrm{Tr}_{L/K}(\mathrm{Tr}_{M/L}(\gamma))$.

7. Пусть $(\alpha_1, \dots, \alpha_n)$, $(\beta_1, \dots, \beta_n)$ — два базиса расширения L/K. Докажите, что $\Delta(\alpha_1, \dots, \alpha_n) = \gamma^2\Delta(\beta_1, \dots, \beta_n)$ для некоторого $\gamma \in K^*$.

8. Пусть $q = p^n$. Докажите, что $\forall a \in \mathbb{F}_p$ уравнение $\mathrm{N}_{\mathbb{F}_q/\mathbb{F}_p}(x) = a$ в $\mathbb{F}_q$ имеет $(p^n-1)/(p-1)$ решений, а также что для каждого $b \in \mathbb{F}_p$ уравнение $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(x) = b$ имеет p^{n-1} решений.

9. Пусть $\mathbb{F}_{q^m}/\mathbb{F}_q$ — расширение конечных полей, $\alpha \in \mathbb{F}_{\|\mathbb{F}\rangle}$. Докажите, что сопряженные элементы $\alpha, \alpha^q, \alpha^{q^2}, \dots \alpha^{q^{m-1}}$ имеют один и тот же порядок в мультипликативной группе $\mathbb{F}^*_{q^m}$.

10. Пусть $\mathbb{F}_{q^m}/\mathbb{F}_q$ — расширение. Докажите, что $\forall c \in \mathbb{F}_q$
$$\sum_{j=0}^{m-1} x^{q^j} - c = \prod_{\alpha \in \mathbb{F}_{q^m}, \mathrm{Tr}(\alpha) = c} (x - \alpha).$$

11. Пусть $\mathbb{F}_{q^m}/\mathbb{F}_q$ — расширение, L — линейный оператор на $\mathbb{F}_{q^m}$ как на векторном пространстве над $\mathbb{F}_q$. Докажите, что $\exists!\alpha_0, \dots, \alpha_{m-1} \in \mathbb{F}_{q^m}$: оператор L имеет вид $L(\beta) = \alpha_0\beta + \alpha_1\beta^q + \dots + \alpha_{m-1}\beta^{q^{m-1}}$.

12. Докажите, что число базисов $\mathbb{F}_{q^m}/\mathbb{F}_q$ равно $(q^m - 1)(q^m - q)\dots(q^m - q^{m-1})$.

13. Пусть $\mathbb{F}_{q^m}/\mathbb{F}_q$ — расширение, $\alpha \in \mathbb{F}_{q^m}$. Докажите, что
$$\Delta(1, \alpha, \dots, \alpha^{m-1}) = \prod_{0 \leqslant i < j \leqslant m-1} (\alpha^{q^i} - \alpha^{q^j})^2.$$

14. Пусть $\mathbb{F}_{q^m}/\mathbb{F}_q$ — расширение, $\alpha \in \mathbb{F}_{q^m}$. Докажите, что $\Delta(1, \alpha, \dots, \alpha^{m-1})$ совпадает с дискриминантом характеристического многочлена $g_\alpha(x)$.

SageMath

- Исследуйте основные функции SageMath связанные с автоморфизмами и расширениями конечных полей:
  - Группа автоморфизмов поля: `End()`;
  - Автоморфизм Фробениуса: `frobenius_endomorphism()`;
  - Базисы расширений конечных полей;
  - Характеристический многочлен `charpoly()`;
  - Норма, след, дискриминант.

Темы для самостоятельного изучения

- Нормальный базис и теорема о нормальном базисе, [LN].

Тема 7. Корни из единицы. Круговой многочлен

Упражнения и задачи

1. Пусть k — поле, $f = a_n x^n + \cdots + a_1 x + a_0 \in k[x]$, $f' = n a_n x^{n-1} + \cdots + a_1 \in k[x]$ — формальная производная f. Докажите следующие свойства:
   - $(f+g)' = f' + g'$;
   - $(fg)' = f'g + fg'$.
2. Пусть k — поле, $f \in k[x]$. докажите, что $\alpha \in k$ — кратный корень $\Leftrightarrow f'(\alpha) = 0$.
3. Пусть $f \in \mathbb{F}_{p^m}[x]$. Докажите, что $f \in \mathbb{F}_p \Leftrightarrow (f(x))^p = f(x^p)$.
4. Докажите, что если $d|n$ и Φ_n определен, то $\Phi_n \mid \dfrac{x^n - 1}{x^d - 1}$.
5. Пусть $f \in \mathbb{F}_q[x]$ — неприводимый, $\deg f = m$. Докажите, что $f \mid x^{q^n} - x \Leftrightarrow m|n$.
6. Докажите, что $\prod' f = x^{q^n} - x$, где произведение берется по всем неприводимым унитарным многочленам $f \in \mathbb{F}_q[x]$ таким, что $\deg f \mid n$. Сделайте вывод о числе неприводимых унитарных многочленов степени d в $\mathbb{F}_q[x]$ (на этот раз для произвольного конечного поля, $q = p^n$).
7. Докажите, что если $\operatorname{char} k = p \not| \, n$, то $\Phi_n = \prod\limits_{d|n} (x^d - 1)^{\mu(n/d)}$.
8. Докажите, что $\mathbb{F}_q$ есть $(q-1)$-е круговое поле над любым своим подполем.
9. Пусть $\alpha \in \mathbb{F}_q$, $n \in \mathbb{Z}$. Докажите, что $x^q - x + \alpha \mid x^{q^n} - x + n\alpha$.
10. Пусть $f \in \mathbb{F}_q[x]$, $q = p^n$. Докажите, что $f'(x) = 0 \Leftrightarrow f = g^p$ для некоторого $g \in \mathbb{F}_q[x]$.
11. Пусть $f \in \mathbb{F}_q[x]$, $q = p^n$, $\deg f = m \geqslant 1$, $f(0) \neq 0$. Докажите, что $\exists e \in \mathbb{Z}_+$ $e \leqslant q^m - 1$ такое что $f(x) \mid x^e - 1$. Наименьшее такое e называется порядком многочлена $f(x)$ в $\mathbb{F}_q[x]$. Докажите также следующие свойства:
    - Пусть $f \in \mathbb{F}_q[x]$ — неприводимый, тогда порядок f равен порядку $\alpha \in \mathbb{F}_{q^m}^*$, α — корень f;
    - Пусть $f \in \mathbb{F}_q[x]$ — неприводимый, тогда порядок f делит $x^e - 1$;
    - Пусть $c \in \mathbb{Z}_+$, e — порядок f, тогда $f(x) \mid x^c - 1 \Leftrightarrow e|c$;
    - Пусть $e_1, e_2 \in \mathbb{Z}_+$, тогда наибольший общий делитель многочленов $x^{e_1} - 1$, $x^{e_2} - 1$ в $\mathbb{F}_q[x]$ равен $x^d - 1$, где $d = (e_1, e_2)$.

SageMath

- Исследуйте основные функции SageMath связанные с работой в кольцах многочленов над конечными полями:
  - Кольцо многочленов: `PolynomialRing()`;
  - Неприводимость многочлена: `is_irreducible()`;
  - Разложение многочлена на множители: `factor()`;

– Корни многочлена: `roots()`;
– Круговой многочлен: `cyclotomic_polynomial()`.

Темы для самостоятельного изучения

- Изучите "элементарные"доказательство неприводимости кругового многочлена $\Phi_n(x)$ в $\mathbb{Z}[x]$. (см. например `https://www.lehigh.edu/ shw2/c-poly/several_proofs.pdf`)

- Теорема Веддербёрна: Всякое конечное кольцо с единицей, в котором каждый ненулевой элемент обратим, является полем. ([LN], [The Book]).

Тема 8. Характеры. Суммы Гаусса

Упражнения и задачи

1. 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 $\forall h \in H$ $\chi(h) = 1$.

2. Пусть G — конечная абелева группа, $\widehat{G}$ — группа характеров, $H < G$ — подгруппа, $A < \widehat{G}$ — аннигилятор H: $A = \{\chi \in \widehat{G} : \forall h \in H\ \chi(h) = 1\}$. Докажите, что $A \cong G/H$ и что $H \cong \widehat{G}/A$.

3. Пусть $G = G_1 \times \cdots \times G_k$ — прямое произведение конечных абелевых групп (множество k-кортежей с операцией $(g_1, \ldots, g_k)(h_1, \ldots, h_k) = (g_1h_1, \ldots, g_kh_k)$). Докажите, что $\widehat{G} \cong \widehat{G_1} \times \cdots \times \widehat{G_k}$.

4. Основная теорема о стуктуре конечных абелевых групп утверждает, что каждая такая группа изоморфна прямому произведению конечного числа циклических групп. Выведете из этой теоремы, что если G — конечная абелева группа, то $\widehat{G} \cong G$.

5. Пусть G – конечная абелева группа, $m > 0$ — целое. Докажите, что $g \in G$ является m-ой степенью в $G \iff \forall$ характера порядка m выполняется $\chi(g) = 1$.

6. Покажите, что для аддитивных характеров ψ_a, ψ_b поля $\mathbb{F}_q$ выполняется $\psi_a\psi_b = \psi_{a+b}$, и что из этого следует изоморфизм аддитивной группы $\mathbb{F}_q$ группе аддитивных характеров поля.

7. Докажите, что для аддитивного характера $\psi = \psi_1$ поля $\mathbb{F}_q/\mathbb{F}_p$ для всех $\alpha \in \mathbb{F}_q$, $j \in \mathbb{Z}_+$ справедливо $\psi_1(\alpha^{p^j}) = \psi_1(\alpha)$.

8. Пусть χ' — мультипликативный характер $\mathbb{F}_{q^s}$ порядка m, χ — ограничение χ' на $\mathbb{F}_q$. Докажите, что χ — мультипликативный характер $\mathbb{F}_q$ порядка $m/(m, (q^s - 1)/(q - 1))$.

9. Пусть χ — мультипликативный характер $\mathbb{F}_q$ порядка, χ' — продолжение χ на $\mathbb{F}_{q^s}$. Докажите, что $\chi'(a) = \chi(q)^s$ $\forall a \in \mathbb{F}_q^*$.

10. Пусть $p \neq 2$, $ab \not\equiv 0\,(p)$, χ — квадратичный характер $\mathbb{F}_p^*$. Докажите, что

- $G(\chi, \psi_a)G(\chi, \psi_b) = \left(\dfrac{-ab}{p}\right) p$;
- $\sum_a G(\chi, \psi_a) = 0$.

11. Пусть $p > 2$, $G = \sum_{x=0}^{p-1} e^{2\pi i x^2/p}$ — сумма Гаусса для квадратичного характера, $A = (a_{st})_{0 \leqslant s,t \leqslant p-1}$ — $p \times p$ матрица с элементами $a_{st} = e^{2\pi i st/p}$. Докажите, что:
    - если $\lambda_0, \ldots, \lambda_{p-1}$ – характеристические числа матрицы A, то $\sum_{k=0}^{p-1} \lambda_k = G$;
    - характеристический многочлен матрицы A^2 имеет вид: $(t-p)^{(p+1)/2}(t+p)^{(p-1)/2}$;
    - для определителя матрицы A справедливо $\det A = i^{p(p-1)/2} p^{p/2}$.

12. Пусть $q = p^n, p > 2$. Определим аналог символа Лежандра для $\mathbb{F}_q$: $\left(\frac{\alpha}{q}\right) = 1$, если α — квадрат в $\mathbb{F}_q$; $\left(\frac{\alpha}{q}\right) = 1$, если α не является квадратом в $\mathbb{F}_q$; $\left(\frac{0}{q}\right) = 0$. Докажите следующие свойства этого символа:
    - $\left(\frac{\alpha\beta}{q}\right) = \left(\frac{\alpha}{q}\right)\left(\frac{\beta}{q}\right)$, $\alpha, \beta \in \mathbb{F}_q$;
    - $\sum_{\alpha \in \mathbb{F}_q} \left(\frac{\alpha}{q}\right) = 0$;
    - $\left(\frac{\alpha}{q}\right) = \left(\frac{\mathrm{N}_{\mathbb{F}_q/\mathbb{F}_p}(\alpha)}{p}\right)$ — обычный символ Лежандра $\pmod p$.

13. Докажите свойства обобщенных сумм Гаусса для конечного подя $\mathbb{F}_q/\mathbb{F}_p$:
    - $G(\chi, \psi_{ab}) = \chi(a)G(\chi, \psi_b)$, $a \in \mathbb{F}_q^*$, $b \in \mathbb{F}_q$;
    - $G(\chi, \bar{\psi}) = \chi(-1)G(\chi, \psi)$;
    - $G(\bar{\chi}, \psi) = \chi(-1)\overline{G(\chi, \psi)}$;
    - $G(\chi, \psi)G(\bar{\chi}, \psi) = \chi(-1)q$, $\chi \neq \chi_0$, $\psi \neq \psi_0$;
    - $G(\chi^p, \psi_b) = G(\chi, \psi_{\sigma(b)})$, $b \in \mathbb{F}_q$, σ — автоморфизм Фробениуса.

14. Пусть $f : \mathbb{F}_q \to \mathbb{C}$, $\hat{f} = \frac{1}{q}\sum_{t \in \mathbb{F}_q} f(t)\overline{\psi(st)}$ — конечное преобрахование Фурье. Докажите, что $f(t) = \sum_{s \in \mathbb{F}_q} \hat{f}(s)\psi(st)$.

SageMath

- Исследуйте основные функции SageMath связанные с группой характеров конечных абелевых групп:
    - `character_table()`.

Темы для самостоятельного изучения

- Докажательство квадратичного закон взаимности через суммы Гаусса. [IR], §7.3; [LN], §5.2.

Тема 9. Тригонометрические суммы. Уравнения над конечными полями

Упражнения и задачи

1. Пусть $F_1(x_1,\dots,x_n),\dots,F_m(x_1,\dots,x_n)$ — многочлены с целыми коэффициентами степеней $r_1,\dots,r_m$. Докажите, что если $r_1+\dots+r_m<n$, то число решений системы сравнений $F_i(x_1,\dots,x_n)\equiv 0\ (p), 1\leqslant i\leqslant m$, делится на p.

2. Пусть p — простое, $F(x_1,\dots,x_n)\in\mathbb{Z}[x_1,\dots,x_n]$ — многочлен с целыми коэффициентами, $\deg F=r<n(p-1)$. Докажите, что $p^a\mid {\sum}' F(x_1,\dots,x_n)$, где в сумме x_i пробегают независимо друг от друга полную систему вычетов $\bmod p$, и $a=n-[r/(p-1)]$.

3. Пусть m — натуральное, $f(x)\in\mathbb{Z}[x]$, $S_a=\sum\limits_{x \bmod m} e^{2\pi i\frac{af(x)}{m}}$. Докажите, что
$$\sum_{a \bmod m}|S_a|^2=m\sum_{c \bmod m}N(c)^2,$$
где $N(c)=N_m\left(f(x)\equiv c\ (m)\right)$ — число решений сравнения $f(x)\equiv c\ (m)$.

4. Пусть p — простое, $S_a=\sum\limits_{x\in\mathbb{F}_p} e^{2\pi i\frac{ax^r}{p}}$, $d=(r,p-1)$. Докажите, что
   - $\sum\limits_{a\in\mathbb{F}_p^*}|S_a|^2=p(p-1)(d-1)$;
   - $|S_a|<d\sqrt{p}$, при $a\neq 0$;
   - и более точная оценка: $|S_a|\leqslant(d-1)\sqrt{p}$, при $a\neq 0$.

5. Пусть χ, λ — неглавные мультипликативные характеры $\mathbb{F}_p$, ϵ — главный, $\tau(\chi)$ — сумма Гаусса. Докажите свойства сумм Якоби:
   - $J(\epsilon,\epsilon)=p$;
   - $J(\epsilon,\chi)=0$;
   - $J(\chi,\chi^{-1})=-\chi(-1)$;
   - $J(\chi,\lambda)=\tau(\chi)\tau(\lambda)/\tau(\chi\lambda)$ при $\chi\lambda\neq\epsilon$.

6. Пусть χ,ρ — мультипликативные характеры $\mathbb{F}_p^*$, χ — неглавный, ρ — порядка 2. Докажите следующие утверждения:
   - $\sum_t\chi(1-t^2)=J(\chi,\rho)$;
   - $\sum_t\chi(t(k-t))=\chi(k^2/4)J(\chi,\rho)$, $k\in\mathbb{F}_p^*$;
   - $G(\chi)^2=\chi(2)^{-2}J(\chi,\rho)G(\chi^2)$ если χ^2 — неглавный;
   - $J(\chi,\chi)=\chi(2)^{-2}J(\chi,\rho)$;
   - если $p\equiv 1\,(4)$, χ — порядка 4, то $\chi^2=\rho$ и $J(\chi,\chi)=\chi(-1)^{-2}J(\chi,\rho)$;
   - $\sum_t\chi(1-t^m)=\sum_{\lambda^m=\epsilon}J(\chi,\lambda)$;
   - $|\sum_t\chi(1-t^m)|\leqslant(m-1)\sqrt{p}$.

7. Пусть $\chi_1,\chi_2,\dots,\chi_l$ — мультипликативные характеры, ε — главный характер $\bmod p$,
   $J=J(\chi_1,\chi_2,\dots,\chi_l)=\sum\limits_{t_1+\dots+t_l=1}\chi_1(t_1)\cdots\chi_l(t_l)$ — обобщенная сумма Якоби,
   $J_0=J_0(\chi_1,\chi_2,\dots,\chi_l)=\sum\limits_{t_1+\dots+t_l=0}\chi_1(t_1)\cdots\chi_l(t_l)$. Докажите следующие свойства J и J_0:

- $J_0(\varepsilon,\dots,\varepsilon) = J(\varepsilon,\dots,\varepsilon) = p^{l-1}$;
- если некоторые, но не все, среди характеров χ_i являются главными, то $J_0 = 0$, $J = 0$;
- пусть $\chi_l \neq \varepsilon$, тогда если $\chi_1\chi_2\cdots\chi_l \neq \varepsilon$, то $J_0 = 0$, а если $\chi_1\chi_2\cdots\chi_l = \varepsilon$, то $J_0(\chi_1,\chi_2,\dots,\chi_l) = \chi_l(-1(p-1))J(\chi_1,\chi_2,\dots,\chi_{l-1})$.

8. Пусть $\chi_1,\chi_2,\dots,\chi_l$ — неглавные характеры $\bmod p$ такие что $\chi_1\chi_2\cdots\chi_l$ тоже неглавный, τ — сумма Гаусса, J — обобщенная сумма Якоби. Докажите, что
   - $\tau(\chi_1)\cdots\tau(\chi_l) = J(\chi_1,\dots,\chi_l)\tau(\chi_1\cdots\chi_l)$;
   - $|J(\chi_1,\dots,\chi_l)| = p^{(l-1)/2}$.

9. Путь $m > 1$ — целое, $K(a,b;m) = \sideset{}{'}\sum_{xy\equiv 1(m)} e^{2\pi i\frac{ax+by}{m}}$, где x пробегает приведеную систему вычетов $\bmod m$. $K(a,b;m)$ называется суммой Клоостермана, удобно также использовать запись $K(a,b;m) = \sideset{}{'}\sum_{x \bmod m} e^{2\pi i\frac{ax+bx^*}{m}}$, где x^* обозначает вычет обратный к x. Докажите следующие свойства сумм Клоостермана:
   - $K(a,b;m) = K(b,a;m)$;
   - если $(m,c) = 1$, то $K(ac,b;m) = K(a,bc;m)$;
   - если $m = m_1m_2$, $(m_1,m_2) = 1$, то $K(a,b;m) = K(n_2a,n_2b;m_1)K(n_1a,n_1b;m_2)$, где n_1,n_2 определены из $m_1n_1 \equiv 1\ (m_2)$, $m_2n_2 \equiv 1\ (m_1)$;
   - если $m = p^{2\alpha}$, $(m,2a) = 1$, то $K(a,a;m) = \sqrt{m}(e^{2\pi i\frac{2a}{m}} + e^{-2\pi i\frac{2a}{m}})$.

10. Пусть p — простое, $(k,p) = 1$, $S = \sideset{}{'}\sum_x\sideset{}{'}\sum_y\left(\frac{xy+k}{p}\right)$, где x,y пробегают возрастающие последовательности из X и Y вычетов полной системы вычетов $\bmod p$. Докажите, что $|S| < \sqrt{XYp}$.

11. Пусть $m > 1$ — целое, $(a,m) = 1$, $S = \sum\limits_{x \bmod m}\sum\limits_{y \bmod m}\xi(x)\eta(y)e^{2\pi i\frac{axy}{m}}$, где ξ,η — такие, что $\sum\limits_{x \bmod m}|\xi(x)|^2 = X$, $\sum\limits_{y \bmod m}|\eta(x)|^2 = Y$. Докажите, что $|S| < \sqrt{XYm}$.

12. Пусть p — простое, $(a,p) = (b,p) = 1$, n — целое $0 < n < p$, $S = \sum\limits_{x\in\mathbb{F}_p^*} e^{2\pi i\frac{ax^n+bx}{p}}$. Докажите, что $|S| < \frac{3}{2}n^{1/4}p^{3/4}$.

13. Пусть $p > 60$ — простое, M,Q — целые, $0 < M < M+Q \leqslant p$, χ — неглавный характер $\bmod p$, $S = \sum\limits_{x=M}^{M+Q-1}\chi(x)$. Докажите, что $|S| < \sqrt{p}\ (\log p - 1)$.

SageMath

- Сопроводите оценки тригонометрических сумм полученные в лекции и упражднениях экспериментальными оценками с помощью SageMath.

Темы для самостоятельного изучения

- Вывод числа решений уравнения $a_1x_1^{l_1} + \cdots + a_rx_r^{l_r} = b$ через суммы Якоби. [IR], глава 8.

- Теорема Бёрджесса. [Степ], §II.1.

Тема 10. Дзета функция Артина

Упражнения и задачи

1. Докажите, что $|\mathbb{P}^n(\mathbb{F}_q)| = q^n + q^{n-1} + \cdots + 1$.

2. Докажите, что для $f = -y_0^2 + y_1^2 + y_2^2 + y_3^2$ дзета-функция имеет вид $Z_f(u) = (1-u)^{-1}(1-qu)^{-2}(1-q^2u)^{-1}$, если -1 — квадрат в $\mathbb{F}_q$, и $Z_f(u) = (1-u)^{-1}(1-qu)^{-1}(1+qu)^{-1}(1-q^2u)^{-1}$ в противном случае.

3. Докажите, что проективная n-мерная гиперплоскость в $\mathbb{P}^n(\mathbb{F}_q)$ (т.е. гиперповерхность, заданная однородным многочленом степени 1) имеет столько же точек сколько $n-1$-мерное проективное пространство $\mathbb{P}^{n-1}(\mathbb{F}_q)$.

4. Пусть $f(x_0, x_1, x_2) \in \mathbb{F}_q[x_0, x_1, x_2]$ — однорлный многочлен $\deg f = n$. $h = \in \mathbb{F}_q[x_0, x_1, x_2]$ — линейная форма, такая что не каждый её нуль является нулём f. Докажите, что в $\mathbb{P}^2(\mathbb{F}_q)$ у f и h может быть не более n общих нулей (т.е. плоская проективная кривая пересекается с проективной прямой в не более чем n точках).

5. Пусть $\mathrm{SL}_n(\mathbb{F}_q)$ — множество $n \times n$ матриц с элементами из поля $\mathbb{F}_q$ и определителем равным 1. Покажите, что $\mathrm{SL}_n(\mathbb{F}_q)$ можно рассматривать как гиперповерхность в $\mathbb{A}^{n^2}(\mathbb{F}_q)$ и что число её точек равно $(q-1)^{-1}(q^n-1)(q^n-q)\ldots(q^n-q^{n-1})$.

6. Пусть $\frac{\partial}{\partial x_i}$ — операторы формальных производных на $\mathbb{F}_q[x_0, \ldots, x_n]$ (например, для $f(x) = a_0x^n + \cdots + a_{n-1}x + a_n$ по определению $\frac{\partial}{\partial x} f = a_0x^{n-1} + \cdots + a_{n-1}$ и пусть $f \in \mathbb{F}_q[x_0, \ldots, x_n]$ — однородный многочлен $\deg f = m$. Докажите, что:
   - $\sum_{i=0}^n x_i \frac{\partial}{\partial x_i} = mf$;
   - если $(m, p) = 1$ ($p = \operatorname{char} \mathbb{F}_q$) и для $a = (a_0, \ldots, a_n)$ при всех i выполняется $\frac{\partial}{\partial x_i} f(a) = 0$, то $f(a) = 0$. (Такая точка a называется особой точкой гиперповерхности $f = 0$).

7. Пусть $q = p^n$, $(m, p) = 1$. Докажите, что гиперповерхность $a_0x_0^m + \cdots + a_nx_n^m = 0$ не имеет особых точек в $\mathbb{P}^n(\mathbb{F}_q)$.

8. Пусть $q = p^n$, $p \neq 2$. Рассмотрим кривую $ax^2 + bxy + cy^22 = 1$, $a, b, c \in \mathbb{F}_q$. 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.

9. Выпишите дзета-функцию кривой $x_0x_1 - x_2x_3 = 0$ над $\mathbb{F}_p$.

10. Выпишите дзета-функцию для $f = a_0x_0^2 + \cdots + a_nx_n^2$ над $\mathbb{F}_q$ при $\mathrm{char}(\mathbb{F}_q) \neq 2$.

11. 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.

12. Выпишите дзета-функцию кривой $y^2 = x^3 + x^2$ над $\mathbb{F}_p$.

13. Пусть $q \equiv 1\,(3)$, $\alpha \in \mathbb{F}_q^*$. Покажите, что дзетв-функция кривой $y^2 = x^3 + \alpha$ над $\mathbb{F}_q$ имеет вид $Z(u) = (1 + au + qu^2)(1 - u)^{-1}(1 - qu)^{-1}$, где $a \in \mathbb{Z}$, $|a| \leqslant 2\sqrt{q}$.

14. Пусть C_1 — кривая над $\mathbb{F}_p$ заданная $y^2 = x^3 - Dx$, $D \neq 0$. Покажите, что подстановка $x = \frac{1}{2}(u + v^2)$, $y = \frac{1}{2}v(u + v^2)$ переводит C_1 в кривую C_2 заданную уравнением $u^2 - v^4 = 4D$. Докажите, что для любого расширения $\mathbb{F}_q/\mathbb{F}_p$ для числа точек справедливо $|C_1(\mathbb{F}_q)| > |C_2(\mathbb{F}_q)|$.

SageMath

- Исследуйте основные функции SageMath связанные с количеством точек на кривых над конечными полями:
  - Для эллиптических и гиперэллиптических кривых: `cardinality()`.

Темы для самостоятельного изучения

- L-функции Артина. Суперэллиптическое уравнение. [Степ], §§I.3–I.4.

Тема 11. p-адические числа: элементарное определение и свойства

Упражнения и задачи

1. Докажите, что различные канонические последовательности определяют различные целые p-адические числа.

2. Докажите, что для целых p-адических чисел α и β заданные в лекции операции $\alpha\beta$, $\alpha + \beta$ корректно определены (то есть результат не зависит от выбора последовательностей-представителей $\alpha \sim (x_n)$, $\beta \sim (y_n)$) и $\mathbb{Z}_p$ — действительно коммутативное кольцо.

3. Пусть $\alpha = \sum_{n=0}^{\infty} a_n p^n \in \mathbb{Z}_p$. Какой будет иметь вид разложение числа $-\alpha$?

4. Докажите, что уравнение $x^2 = 2$ не имеет решений в $\mathbb{Q}_5$.

5. Докажите, что $\forall \alpha \in \mathbb{Z}_p\ \exists a \in \mathbb{Z}:\ \alpha \equiv a \pmod{p^n}$. Для $a, b \in \mathbb{Z}$ $a \equiv b \pmod{p^n}$ как сравнение в $\mathbb{Z}_p \Leftrightarrow a \equiv b \pmod{p^n}$ как сравнение в $\mathbb{Z}$.

6. Пусть $p \neq 2$, $(m, p) = 1$. Сформулируйте и докажите необходимое и достаточное условие разрешимости уравнения $x^2 = m$ в $\mathbb{Q}_p$. Сделайте вывод, что $\mathbb{Q}_p$ не является алгебраически замкнутым.

7. Докажите, что если $\xi_n \to \xi$ в $\mathbb{Q}_p$ и $\xi \neq 0$, то $1/\xi_n \to 1/\xi$ в $\mathbb{Q}_p$.

8. Докажите p-адический аналог утверждения из анализа: из всякой ограниченной последовательности можно выделить сходящуюся подпоследовательность.

9. Докажите p-адический критерий Коши: последовательность (ξ_n) сходится $\Leftrightarrow$ $\nu_p(\xi_m - \xi_n) \to \infty$, при $m, n \to \infty$.

10. Пусть последовательность (x_n) определена как $x_n = 1 + p + \cdots + p^{n-1}$. Докажите, что в $\mathbb{Q}_p$ $x_n \to 1/(1 - p)$, $n \to \infty$.

11. Докажите, что для $0 \neq \xi \in \mathbb{Q}_p \cap \mathbb{Q}$ представление $\xi = \sum_{n=0}^{\infty} a_n p^n$, $0 \leqslant a_n \leqslant p-1$ имеет периодические коэффициенты (начиная с некоторого номера k_0, т.е. $\exists m$: $\forall k \geq k_0\ a_{m+k} = a_k$). Обратно всякий такой ряд представляет рациональное число.

SageMath

- Исследуйте основные функции SageMath связанные с арифметикой p-адических чисел. Определение кольца и поле p-адических чисел: `Zp(n)`, `Qp(n)`. Рассмотрите примеры уравнения $x^2 = m$ (используйте функцию `sqrt()`).

Темы для самостоятельного изучения

- Элементы p-адического анализа: последовательности, ряды, дифференцирование, интегрирование. [Gouv], §§5.1–5.4.

Тема 12. Аксиоматическое определение поля p-адических чисел, метризованные поля

Упражнения и задачи

1. Пусть (k, φ) — метризованное поле. Докажите следующие свойства:
   - $\varphi(\pm 1) = 1$; $\varphi(-x) = \varphi(x)$;
   - $\varphi(x - y) \leqslant \varphi(x) + \varphi(y)$;
   - $\varphi(x \pm y) \geqslant |\varphi(x) - \varphi(y)|$;
   - $\varphi(x/y) = \varphi(x)/\varphi(y)$, $y \neq 0$.

2. Пусть (k, φ) — метризованное поле, d — индуцированное расстояние: $d(x, y) = \varphi(x - y)$. Докажите, что операции поля $(+, -, \cdot, /)$ являются непрерывными по отношению к d (то есть k — топологическое поле).

3. Пусть (k, φ) — метризованное поле. Докажите, что $\lim\limits_{n\to\infty} x_n = x \Leftrightarrow$ каждое открытое множество содержащее x содержит все кроме конечного числа элементы последовательности x_n.

4. Пусть k — поле, на котором заданы две метрики (абсолютные величины) φ_1, φ_2. Докажите следующие импликации теоремы о критериях эквивалентности:
   - φ_1, φ_2 — эквивалентны $\implies$ для любой сходящейся последовательности $\lim\limits_{n\to\infty}{}^{(\varphi_1)} x_n = x$ если и только если $\lim\limits_{n\to\infty}{}^{(\varphi_2)} x_n = x$ ($\lim^{(\varphi)}$ означает предел по метрике φ);
   - $\lim\limits_{n\to\infty}{}^{(\varphi_1)} x_n = \lim\limits_{n\to\infty}{}^{(\varphi_2)} x_n = x \implies \forall x \in k\ \varphi_1(x) < 1$ если и только если $\varphi_2(x) < 1$;
   - $\exists \alpha \in \mathbb{R}$: $\forall x \in k\ \varphi_1(x) = \varphi_2(x)^\alpha \implies \varphi_1$, φ_2 эквивалентны.

5. Пусть k — поле, φ — функция $k \to \mathbb{R}_{>0}$ такая что:
   - $\varphi(x) = 0 \Leftrightarrow x = 0$,
   - $\varphi(xy) = \varphi(x)\varphi(y)$,
   - $\varphi(x) \leqslant 1 \Rightarrow \varphi(x - 1) \leqslant 1$.

Докажите, что φ является неархимедовой метрикой на k.

6. Пусть (k, φ) — метризованное поле , φ — неархимедова метрика. Докажите, что $\varphi(x) \neq \varphi(y) \Rightarrow \varphi(x+y) = \max(\varphi(x), \varphi(y))$.

7. Пусть (k, φ) — метризованное поле, A — образ $\mathbb{Z}$ в k. Докажите, что φ — неархимедова метрика $\Leftrightarrow \forall a \in A\ \varphi(a) \leqslant 1$. (Подсказка: сведите к утверждению φ — неархимедова метрика $\Leftrightarrow \varphi(x+1) \leqslant \max(\varphi(x), 1)$; рассмотрите $\varphi(x+1)$).

8. Пусть (k, φ) — метризованное поле, φ — неархимедова метрика, $B(x, r)$ — открытый шар радиуса r с центром в x. Докажите следующие свойства:
   - $\forall y \in B(x, r)\ B(x, r) = B(y, r)$;
   - $\partial B(x, r) = \varnothing$ ($\partial B(x, r)$ обозначает множество граничных точек);
   - $B(x, r) \cap B(y, s) \neq \varnothing \Leftrightarrow B(x, r) \subset B(y, s)$ или $B(y, s) \subset B(x, r)$.

   Рассмотрите аналогичные утверждения для замкнутых шаров $\bar{B}(x, r)$.

9. Пусть $\operatorname{char} k = p$. Докажите, что всякая метрика φ поля k неархимедова.

10. Пусть k — поле, $k(t) = \{f(t)/g(t) : f, g \in k[t], g \neq 0\}$ — поле рациональных функций над k. $\forall r \in k(t)^*$ определим $\varphi(r) = \rho^m$, где m такое, что $r = f/g = t^m(f_0/g_0)$, где f_0, g_0 не делятся на t как многочлены, $0 < \rho < 1$; для $r = 0$ положим $\varphi(0) = 0$. Докажите, что ϕ — метрика поля $k(t)$.

    Докажите, что множество 2-адических чисел $\mathbb{Z}_2$ с 2-адической метрикой $|\cdot|_2$ гомеоморфно Канторову множеству C с обычным модулем $|\cdot| = |\cdot|_\infty$.

SageMath

- В контексте задач 11 и 12 ознакомьтесь с функцией `Zp(n).plot()`.

Темы для самостоятельного изучения

- Единственность пополнения поля по метрике. [БШ] §I.4.
- $\forall$ простого p множество целых p-адических чисел $\mathbb{Z}_p$ гомеоморфно множеству 2-адических чисел $\mathbb{Z}_2$. [Kat], глава 2.

Тема 13. Лемма Гензеля, принцип Хассе

Упражнения и задачи

1. Пусть k — произвольное поле, $F(X) \in k[x]$. Докажите формулу Тейлора для формальной производной F'.

2. Докажите, что порядок фактор группы $\mathbb{Q}_2^*/(\mathbb{Q}_2^*)^2$ равен 8. Укажите соответствующее множество представителей.

3. Пусть $p \neq 2$, $\alpha, \beta \in \mathbb{Z}_p$, $p \nmid \alpha, p \nmid \beta$. Докажите, что разрешимость сравнения $\alpha x^p \equiv \beta \pmod{p^2}$ достаточна для разрешимости уравнения $\alpha x^p = \beta$ в $\mathbb{Q}_p$.

4. Пусть $p \neq 2, U = U(\mathbb{Z}_p)$ — группа p-адических единиц, $U_n = 1 + p^n\mathbb{Z}_p$. ($U_n = \{\alpha \in \mathbb{Z}_p : \nu_p(\alpha - 1) \geqslant n\}$, т.е. U_n — p-адические окрестности единичного элемента). Докажите следующие свойства:

- $U_n/U_{n+1} = \mathbb{Z}/p\mathbb{Z}$, $U = \varprojlim U_n$;
- $U = U_1 V$, где V — циклическая подгруппа корней степени $p-1$ из единицы;
- Если $\alpha \in U_n \setminus U_{n+1}$, то $\alpha^p \in U_{n+1} \setminus U_{n+2}$;
- U_1/U_n — циклическая группа, $U_1 \cong \mathbb{Z}_p$.

Сделайте вывод о структуре мультипликативной группы $\mathbb{Q}_p$: $\mathbb{Q}_p^* \cong \mathbb{Z} \times \mathbb{Z}_p \times \mathbb{Z}/(p-1)\mathbb{Z}$.

5. Пусть $F(x_1, \ldots, x_n) \in \mathbb{Z}_p[x_1, \ldots, x_n]$, N_m — число решений сравнения $F \equiv 0 \pmod{p^m}$, $L_F(u) = \sum_{m=0}^{\infty} N_m u^m$ — так называемый ряд Пуанкаре (вспомните дзета функцию Артина).
   - Найдите ряд Пуанкаре для $F = \alpha_1 x_1 + \cdots + \alpha_n x_n$, где $\alpha_i \in \mathbb{Z}_p^*$. Убедитесь, что в этом случае $L_F(u)$ — рациональная функция.
   - Найдите ряд Пуанкаре для многочлена $F(x_1, \ldots, x_n)$, обладающего свойством: для всякого решения сравнения $F(x_1, \ldots, x_n) \equiv 0 \pmod{p}$ при некотором i имеем $F'_{x_i}(x_1, \ldots, x_n) \not\equiv 0 \pmod{p}$;
   - Найдите ряд Пуанкаре для $F(x, y) = x^2 - y^3$;
   - Докажите рациональность ряда Пуанкаре для многочленов одной переменной.

   (Существует теорема (Игусы) о том, что L_F всегда является рациональной функцией).

6. Докажите p-адический критерий Эйзенштейна: пусть $f \in \mathbb{Z}_p[x]$, $f(x) = a_0 x^n + \ldots a_n$, f – неприводим, если $p \nmid a_0$, $p \mid a_i$ $1 \leqslant i \leqslant n$, $p^2 \nmid a_n$.

7. Верно ли следующее: $f \in \mathbb{Z}[x]$ неприводим в $f \in \mathbb{Q}[x] \Leftrightarrow f$ неприводим в $\mathbb{Q}_p[x]$ $\forall p \leqslant \infty$?

8. Докажите, что уравнение $(x^2-2)(x^2-17)(x^2-34) = 0$ разрешимо в $\mathbb{Q}_p$ $\forall p \leqslant \infty$ но не разрешимо в $\mathbb{Q}$.

SageMath

- Исследуйте функции SageMath для работы с многочленами с p-адическими коэффициентами:
  - Разложение многочлена: `factor()`.
  - В контексте Леммы Гензеля: `hensel_lift()`.

Темы для самостоятельного изучения

- Разрешимость уравнений с квадратичными формами над полем p-адических чисел ([БШ §I.6 п.2).
- Приложение теоремы Минковского-Хассе для квадратичной формы от трёх переменных ([Gouv §4.8]).

Тема 14. Кольцо целых гауссовых чисел

Упражнения и задачи

1. Пусть R — евклидово кольцо (с нормой $N(\cdot)$). Докажите, что u — единица $R \iff N(u) = 1$.

2. Пусть R — кольцо. Докажите следующие утверждения (свойства делимости на языке идеалов):
   - $a|b \Leftrightarrow (b) \subseteq (a)$;
   - u — единица $\Leftrightarrow (u) = R$;
   - a, b — ассоциированы $\Leftrightarrow (a) = (b)$;
   - p — простой элемент $\Leftrightarrow ab \in (p) \Rightarrow a \in (p)$ или $b \in (p)$;
   - p — неприводимый элемент $\Leftrightarrow (p) \subseteq (a) \Rightarrow (a) = R$ или $(a) = (p)$.

3. Пусть R — кольцо главных идеалов, $a, b \in R$ d — НОД a, b. Докажите, что $\exists d \in R : (d) = (a, b)$.

4. Пусть R — кольцо главных идеалов. Докажите, что $p \in R$ — неприводимый элемент $\iff$ p — простой.

5. Докажите свойство показателя в кольце главных идеалов: если p — неприводимый элемент, $a, b \in R^*$, то $\nu_p(ab) = \nu_p(a) + \nu_p(b)$.

6. Докажите теорему об однозначности разложения на простые множители в кольцах главных идеалов.

7. Пусть $\pi \in \mathbb{Z}[i]$ — простой элемент, $\nu_\pi(\alpha)$ — соответствующий показатель, $|\alpha|_\pi = (\mathrm{N}\, p)^{-\nu_\pi(\alpha)}$ — метрика заданная на $\mathbb{Z}[i]$ и $\mathbb{Q}(i)$. Опишите ограничение этой метрики на $\mathbb{Q}$.

8. Докажите, что $\mathbb{Z}[\omega]$ — евклидово кольцо. Найдите единицы $\mathbb{Z}[\omega]$.

9. Докажите, что для функций определенных в лекции выполняется $d(n_1) = d_1(n) - d_3(n)$.

10. Докажите оценку для числа представлений в виде суммы двух квадратов: $r_2(n) = \mathcal{O}_\varepsilon(n^\varepsilon)$.

SageMath

- Рассмотрите примеры арифметики кольца гауссовых чисел: `ZZ[I]`, исследуйте базовые функции такие как `gcd(), xgcd(), factor(), ...`.

- Исследуйте функции для нахождения разложений целых чисел в виде суммы двух и четырёх квадратов, например, библиотека `sum_of_squares`.

Темы для самостоятельного изучения

- Арифметика кольца чисел Эйзенштейна $\mathbb{Z}[\omega]$, [IR], §§9.1–9.2.

- Алгебра кватернионов, число представлений суммой четырёх квадратов, [DSV], §§2.5–2.6.

Тема 15. Арифметика колец целых алгебраических чисел

Упражнения и задачи

1. Докажите, что $r \in \mathbb{Q}$ — целое алгебраическое число $\iff$ $r \in \mathbb{Z}$.

2. Пусть $\omega_1, \ldots, \omega_l$ — целые алгебраические числа, $W = \{\sum_{i=1}^{l} r_i\omega_i : r_i \in \mathbb{Z}\}$. Докажите, что
   - W — конечно порождённый модуль над $\mathbb{Z}$;
   - если для $\omega \in \mathbb{C}$ верно $\forall \gamma \in W\ \gamma\omega \in W$, то ω — целое алгебраическое число;
   - множество целых алгебраических чисел является кольцом.

3. Докажите, что если α — целое алгебраическое, то $\mathbb{Q}(\alpha) = \mathbb{Q}[\alpha]$.

4. Пусть $K/\mathbb{Q}$ — числовое поле, $\mathcal{D}_K$ — кольцо целых. Докажите, что
   - $\mathrm{N}_{K/\mathbb{Q}}(\alpha), \mathrm{Tr}_{K/\mathbb{Q}}(\alpha) \in \mathbb{Z}\ \forall \alpha \in \mathcal{D}_K$;
   - если $\alpha_1, \ldots, \alpha_n \in \mathcal{D}_K$ — базис расширения, то $\Delta(\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}$.

5. Пусть $I \subset \mathcal{D}_K$ — идеал. Докажите, что если $\alpha_1, \ldots, \alpha_n \in I$ — базис расширения $K/\mathbb{Q}$ такой, что $\Delta(\alpha_1, \ldots, \alpha_n)$ минимален, то $I = \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_n$.

6. Покажите, что 3, 7, $1 + 2\sqrt{-5}$, $1 - 2\sqrt{-5}$ являются простыми в $\mathbb{Z}[\sqrt{-5}]$ (т.о. $21 = 3 \cdot 7 = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5})$ — пример неоднозначного разложения на простые множители).

7. Докажите, что кольцо целых $\mathcal{D}_K$ является нётеровым, и что всякий простой идеал $P \subset \mathcal{D}_K$ является максимальным.

8. Докажите, что $h_K = 1 \iff \mathcal{D}_K$ — кольцо главных идеалов.

9. Докажите следующие свойства идеалов $\mathcal{D}_K$:
   - $AB = AC \implies B = C$;
   - $A \subset B \implies \exists C\colon A = BC$.

10. Докажите следующие свойства функции показателя:
    - $\nu_P(P) = 1$;
    - $P_1 \neq P_2 \implies \nu_{P_1}(P_2) = 0$;
    - $\nu_P(AB) = \nu_P(A)\nu_P(B)$.

11. Завершите доказательство теоремы об однозначности разложения идеалов кольца $\mathcal{D}_K$.

12. Пусть P — простой идеал $\mathcal{D}_K$. Докажите, что $\mathcal{D}_K/P$ является конечным полем.

13. Пусть R — коммутативное кольцо с единицей, $A_1, \ldots, A_g \subset R$ — идеалы такие, что $A = A_1 \cdot \cdots \cdot A_g$ и $\forall i \neq j\ A_i + A_j = R$. Докажите, что $R/A \cong R/A_1 \oplus \cdots \oplus R/A_g$.

14. Пусть $P, Q \subset \mathcal{D}_K$ — простые идеалы. Докажите, что $\forall m, n \in \mathbb{Z}_+\ P^m + Q^n = \mathcal{D}_K$.

Темы для самостоятельного изучения

- Теория Галуа для случая числовых полей, [Marc], Appendix B.

Тема 16. Квадратичное поле и круговое поле

Упражнения и задачи

1. Пусть $\mathcal{D}$ — кольцо целых квадратичного поля $\mathbb{Q}(\sqrt{d})$. Докажите, что $\mathcal{D} = \mathbb{Z}[\sqrt{d}]$ при $d \equiv 2, 3\,(4)$ и $\mathcal{D} = \mathbb{Z}\left[\frac{-1+\sqrt{d}}{2}\right]$ при $d \equiv 1\,(4)$.

2. Пусть ζ — примитивные корень степени m из единицы. Докажите, что $\Delta(1, \zeta, \ldots, \zeta^{\varphi(m)-1}) | m^{\varphi(m)}$.

3. Докажите, что числовое поле нечетной степени не может содержать примитивных корней из единицы степени $n > 2$

4. Пусть K — вещественное квадратичное поле (т.е. $K \subset \mathbb{R}$). Докажите, что если $\exists \alpha \in K$: $\mathrm{N}(\alpha) = -1$, то простые $p \equiv 3\,(4)$ не разветвляются.

5. Пусть K — вещественное квадратичное поле такое что $\zeta_n \in K$ для некоторого $n \geqslant 3$. Докажите, что $\forall \alpha \in F^*$ $\mathrm{N}(\alpha) > 0$.

6. Докажите, что квадратичное поле K не может одновременно содержать $\sqrt{p}$, $\sqrt{q}$ для двух различных простых p, q.

7. Пусть K — вещественное квадратичное поле. Докажите, что $\forall M > 0$ $\exists \beta \in \mathcal{D}_K$: $|1 - \beta| > M$, а также что $\forall \varepsilon > 0$ $\exists \alpha \in \mathcal{D}_K$: $|1 - \alpha| < \varepsilon$.

8. Пусть $p > 2$ — простое, $\zeta = \zeta_p$, $K = \mathbb{Q}(\zeta_p)$. Докажите следующие свойства:
   - $\mathrm{N}_{K/\mathbb{Q}}(1 + \zeta) = 1$;
   - $A = \prod_{(s/p)=1}(1 + \zeta^s) \in \mathbb{Q}(\sqrt{p})$;
   - если $p \equiv 1\,(4)$, то $A = \frac{1}{2}(t + u\sqrt{p})$, где $t \equiv u\,(2)$;
   - $\left(\dfrac{t^2 - pu^2}{4}\right)^{\frac{p-1}{2}} = 1$; $t^2 - pu^2 = \pm 4$;
   - $A > 0$.

9. Для каких d квадратичное поле $\mathbb{Q}(\sqrt{d})$ имеет базис вида α, α'?

10. Пусть $\zeta = e^{2\pi i/5}$, $K = \mathbb{Q}(\zeta)$. Покажите, что $-(\zeta^3 + \zeta^2) \in \mathcal{U}_{\mathcal{D}_K}$.

11. Пусть $K = \mathbb{Q}(\zeta_p)$. Покажите, что $\frac{\sin(\pi j/p)}{\sin(\pi/p)} \in \mathcal{U}_{\mathcal{D}_K}$.

12. Пусть $p \equiv 1\,(4)$, $K = \mathbb{Q}(\zeta_p)$. Докажите, что группа единиц $\mathcal{U}_{\mathcal{D}_K}$ бесконечна

13. Докажите, что всякое квадратичное поле содержится в некотором круговом поле.

Темы для самостоятельного изучения

- Арифметика кольца целых кругового поля, приложения к доказательству квадратичного закона взаимности, [IR], §§13.2–13.3.

- Порядки числовых полей, [БШ]; [Cox].

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	1 (1.1)
2	Мультипликативные функции, функции Эйлера и Мёбиуса. Формула обращения Мёбиуса	1 (1.1)
3	Неравенства Чебышева	1 (1.1)
4	Сравнения, полная и приведенная система вычетов. Число решений линейного сравнения. Теоремы Эйлера и Ферма	2 (1.2)
5	Китайская теорема об остатках	2 (1.2)
6	Однозначность разложения в кольце многочленов	2 (1.2)
7	Теорема Лагранжа о числе корней многочлена. Теорема Вильсона	3 (1.3)
8	Первообразные корни и структура группы единиц по модулю m	3 (1.3)
9	Степенные вычеты	3 (1.3)
10	Квадратичные вычеты, символ Лежандра и его свойства	4 (1.4)
11	Квадратичный закон взаимности	4 (1.4)
12	Сравнения по двойному модулю, существование неприводимых многочленов произвольной степени над конечным полем	5 (2.1)
13	Мультипликативная группа конечного поля	5 (2.1)
14	Автоморфизм Фробениуса, группа Галуа конечного поля	5 (2.1)
15	Круговое поле, группа корней из единицы	6 (2.2)
16	Круговой многочлен, разложение кругового многочлена на неприводимые множители над конечным полем	6 (2.2)
17	Норма и след, их свойства. Абсолютные и относительные норма и след	7 (2.3)
18	Характеры абелевых групп	7 (2.3)
19	Сумма Гаусса, значение её модуля	7 (2.3)
20	Теоремы Варинга и Шевалле	8 (2.4)
21	Теорема Виноградова-Пойя	8 (2.4)
22	Суммы Якоби и их свойства	8 (2.4)

№	Вопрос	Раздел и тема дисциплины
23	Аффинное и проективное пространства над конечным полем	9 (2.5)
24	Соотношение Хассе-Дэвенпорта	9 (2.5)
25	Дзета функция Артина, критерий её рациональности	9 (2.5)
26	Построение кольца целых p-адических чисел	10 (3.1)
27	Делимость и единицы в кольце целых p-адических чисел, p-показатель и p-адическая метрика	10 (3.1)
28	Ряды и последовательности p-адических чисел, их сходимость	10 (3.1)
29	Метризованные поля, эквивалентность метрик пополнение по метрике	11 (3.2)
30	Теорема Островского	11 (3.2)
31	Неархимедовы метрики и их топологические свойства	11 (3.2)
32	Кольцо и идеал показателя. Локальные кольца	12 (3.3)
33	Лемма Гензеля	12 (3.3)
34	Делимость и разложение на множители в кольцах $\mathbb{Z}[i]$, $\mathbb{Z}[\omega]$	13 (4.1)
35	Кубический и биквадртичный характеры. Высшие законы взаимности	13 (4.1)
36	Числовые поля. Норма, след и дискриминант	14 (4.2)
37	Дедекиндовы кольца, однозначность разложения на простые идеалы	14 (4.2)
38	Квадратичное поле и его кольцо целых. Порядки в квадратичном поле	15 (4.3)
39	Круговое поле и его кольцо целых. Круговой многочлен	15 (4.3)

Примеры контрольных задач приведены в разделе 5.3.

7 Ресурсное обеспечение

7.1 Перечень основной и дополнительной литературы

Список литературы

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

[IR] 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).

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

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

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

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

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

[Marc] D.A. Marcus, Number Fields. Springer, 2018.

[Cox] D.A. Cox, Primes of the Form x2+ny2. Wiley, 2013.

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

[Stein-ent] W. Stein, Elementary Number Theory: Primes, Congruences, and Secrets, 2017.

[Kat] S. Katok, p-adic Analysis Compared with Real. AMS, 2007 (С.Б. Каток, p-адический анализ в сравнении с вещественным. МЦНМО, 2004).

7.2 Перечень лицензионного программного обеспечения, в том числе отечественного производства

При реализации дисциплины может быть использовано следующее программное обеспечение:

- Операционная система Linux (Свободно-распространяемое ПО) / MacOS / Windows;
- Язык программирования Python и система компьютерной алгебры SageMath. Свободно-распространяемое ПО;
- Среда разработки Jupyter / VS Code / Vim (Emacs), ... Свободно-распространяемое ПО;
- Издательская система LaTeX. Свободно-распространяемое ПО.

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.

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 луч-

ше 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 рекомен-

дуется 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.