

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):
Решётки и формы

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	3
2 Цели и задачи дисциплины	3
3 Результаты обучения по дисциплине (модулю)	3
4 Формат обучения и объём дисциплины (модуля)	4
5 Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведённого на них количества академических часов и видов учебных занятий	5
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)	5
5.2 Содержание разделов (тем) дисциплины	6
5.3 Примеры задач для семинаров и самостоятельной работы	8
6 Фонд оценочных средств (ФОС, оценочные и методические материалы) для оценивания результатов обучения по дисциплине (модулю)	10
6.1 Типовые контрольные задания или иные материалы для проведения текущего контроля успеваемости	10
7 Ресурсное обеспечение	11
7.1 Перечень основной и дополнительной литературы	11
7.2 Перечень лицензионного программного обеспечения, в том числе отечественного производства	12
7.3 Перечень профессиональных баз данных и информационных справочных систем	13
7.4 Перечень ресурсов информационно-телекоммуникационной сети «Интернет»	13
7.5 Описание материально-технического обеспечения	13
8 Методические рекомендации по организации изучения дисциплины	14
8.1 Формы и методы преподавания дисциплины	14
8.2 Методические рекомендации преподавателю	14
8.3 Методические рекомендации студентам по организации самостоятельной работы	16

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 алгебры, теории чисел, действительного и комплексного анализа, а также владеющих основами языка программирования Python.

2 ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

В курсе рассматриваются математические концепции и структуры, возникающие при изучении евклидовых решёток. Евклидовы решётки находят широкое применение как в чистой математике (теория чисел, алгебра и теория представлений, геометрия и топология, комбинаторика, ...), так и в прикладной (коды исправляющие ошибки, криптография и криптоанализ, математическая оптимизация и целочисленное программирование, дизайн экспериментов, кристаллография, ...). Важным способом описания и решения задач теории решёток является теория целых квадратичных форм. С евклидовой решёткой и целой квадратичной формой может быть ассоциирована функция комплексного переменного специального вида, называемая тета-функцией. Эта тета-функция является модулярной формой, а теория модулярных форм позволяет получать глубокие результаты относительно свойств как самой тета-функции, так и связанных с ней решёткой и квадратичной формой. Например, через значения и параметры тета-функции могут быть выражены инварианты целых квадратичных форм и, как следствие, инварианты евклидовых решёток. В свою очередь теория модулярных и автоморфных форм находит применение практически во всех разделах современной математики и представляет интерес сама по себе. Цель курса: познакомить слушателей с основными определениями и результатами из трёх разделов теории чисел: 1) евклидовы решётки, 2) целые квадратичные формы, 3) модулярные формы, показать фундаментальную связь этих разделов между собой и обозначить направления приложения этих теорий в других разделах математики и кибернетики.

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-ВТЧПРФ-1М.1.** Знакомство с основными понятиями и методами теории евклидовых решёток.
- **СПК-ВТЧПРФ-1М.2.** Знакомство с основными понятиями и методами теории целых квадратичных форм.
- **СПК-ВТЧПРФ-1М.3.** Знакомство с основными понятиями и методами теории модулярных форм.
- **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 теории евклидовых решёток;
 - Основные понятия, определения и результаты теории целых квадратичных форм;
 - Основные понятия, определения и результаты теории модулярных форм;
 - 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 96 академических часов, в том числе 48 академических часов, отведенных на контактную работу обучающихся с преподавателем, 48 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 трудо-затраты обучающегося, академические часы					
Наименование разделов и тем дисциплины (модуля), Форма промежуточной аттестации по дисциплине (модулю)	Кон-тактная работа, занятия лекционного типа	Кон-тактная работа, занятия семинарского типа	Самостоятельная работа обучающегося	Всего академических часов	Форма текущего контроля успеваемости* (наименование)	
<i>Раздел 1. Евклидовы решётки и квадратичные формы</i>						
Тема 1. Евклидовы решётки: основные определения и свойства	2	2	4	8		
Тема 2. Лемма Минковского	2	2	4	8		
Тема 3. Группа единиц целых алгебраических чисел	2	2	4	8		
Тема 4. Квадратичные формы: элементы общей теории	2	2	4	8		
Тема 5. Целые квадратичные формы	2	2	4	8		
Тема 6. Решётки корней	2	2	4	8		
Тема 7. Бинарные квадратичные формы	2	2	4	8		
<i>Раздел 2. Модуллярные формы</i>						
Тема 8. Модуллярные формы: основные определения и примеры	2	2	4	8		

Тема 9. Алгебра модулярных форм	2	2	4	8	
Тема 10. Тета-функции	2	2	4	8	
Тема 11. Операторы Гекке и L-функции модулярных форм	2	2	4	8	
Тема 12. Модулярные формы для конгруэнц подгрупп и модулярные формы полуцелых весов	2	2	4	8	
Итоговая аттестация					экзамен
Итого, академические часы	24	24	48	96	

5.2 Содержание разделов (тем) дисциплины

Курс состоит из двух разделов: первый раздел посвящён евклидовым решёткам и целым квадратичным формам, во втором разделе рассматриваются классические модулярные формы и некоторые их приложения.

Наименование разделов (тем) дисциплины	Содержание разделов (тем) дисциплин
<i>Раздел 1. Евклидовые решётки и квадратичные формы</i>	
Тема 1. Евклидовые решётки: основные определения и свойства.	Евклидовые решётки и подрешётки. Размерность и ранг. Свойства дискретности, теорема Бибербаха. Основной параллелепипед. Объем и дискриминант. <i>Источники:</i> [БШ], параграф II.3; [GM], глава 1; первые лекции в [Micc-LN], [Peik-LN], [Roth-LN].
Тема 2. Лемма Минковского.	Выпуклость. Лемма Минковского и ее варианты. Последовательные минимумы решётки. Теорема Бликфельдта. Двойственные и унимодулярные решётки. Некоторые теоретико-числовые приложения. <i>Источники:</i> [БШ], параграф II.3; [Cass], глава 5; [GM], глава 1; [Galb], глава 16; первые лекции в [Micc-LN], [Peik-LN], [Roth-LN].
Тема 3. Группа единиц целых алгебраических чисел.	Геометрическое изображение алгебраических чисел. Образ кольца целых как решётка. Теорема Дирихле о структуре группы единиц кольца целых. Порядки числовых полей (обзорно). Приложение к представимости квадратичными формам (обзорно). <i>Источники:</i> [БШ], глава 3.

Тема 4. Квадратичные формы: элементы общей теории.	Билинейные и квадратичные формы над произвольным полем. Эквивалентность квадратичных форм. Диагонализация. Прямая сумма и теорема Витта. Группа Витта. Основные инварианты квадратичных форм (обзорно). Классификация квадратичных форм над полями рациональных, действительных и p -адических чисел (обзорно), представимость элементов поля квадратичными формами. <i>Источники:</i> [Serre], глава IV; [БШ], дополнение, параграф 1; [Cass], глава 2; [Schulze-LN]; [Clark-LN].
Тема 5. Целые квадратичные формы.	Квадратичный модуль. Целочисленная эквивалентность квадратичных форм, связь с евклидовыми решётками. Группа Гортендика. Инварианты и критерии для эквивалентности целых квадратичных форм (обзорно). Локальные (p -адические) и глобальные (целые) свойства решёток. <i>Источники:</i> [Serre], глава V; [Cass], главы 7-11; [CS], глава 15.
Тема 6. Решётки корней.	Понятие решётки корней. Фундаментальная система корней. Теорема Витта о существовании нормированной фундаментальной системы корней. Диаграммы Коксетера-Дынькина. Приводимые и неприводимые решётки корней, классификация неприводимых решёток, теорема о разложении произвольных решёток корней в прямую сумму неприводимых. <i>Источники:</i> [Eb], параграфы 1.4-1.5; [Serre], глава V.
<i>Раздел 2. Модулярные формы</i>	
Тема 8. Модулярные формы: основные определения и примеры.	Слабомодулярные и модулярные функции. Модулярные и параболические формы. Примеры модулярных форм: ряды Эйзенштейна и модулярный дискриминант. <i>Источники:</i> [Serre], глава VII; [Eb], параграфы 2.2, 2.5.
Тема 9. Алгебра модулярных форм.	Нули и полюса модулярных функций. Размерность и структура пространства модулярных форм. Алгебра модулярных форм. Модулярный инвариант. Некоторые явные формулы и соотношения для коэффициентов Фурье модулярных форм. <i>Источники:</i> [Serre], глава VII; [Eb], параграф 2.6; [Kob], параграфы III.1-III.2.
Тема 10. Тета-функции.	Формула суммирования Пуассона. Тета-функция решётки как модулярная форма. Свойства унимодулярных решёток. Единственность решётки E_8 . Решётка Лича (обзорно). Некоторые результаты и формулы для числа представлений суммами квадратов и целыми квадратичными формами. <i>Источники:</i> [Serre], параграф VII.6; [Eb], глава 2.

Тема 11. Операторы Гекке и L-функции модулярных форм.	Операторы Гекке, коммутативность алгебры операторов Гекке. Действие операторов Гекке на модулярные функции и формы. Свойства коэффициентов модулярных форм. Скалярное произведение Петерсона. Собственные значения и собственные функции операторов Гекке. Оценки коэффициентов модулярных форм. L-функции модулярных форм, аналитическое продолжение и функциональное уравнение. <i>Источники:</i> [Serre], параграф VII.5; [Iw], параграф 6.4, глава 7; [Kob], параграф III.5; [Bump], параграфы 1.3-1.4.
Тема 12. Модулярные формы для конгруэнц подгрупп и модулярные формы полуцелых весов.	Конгруэнц подгруппы полной модулярной группы. Модулярные формы для конгруэнц подгрупп. Модулярные формы полуцелых весов. Характеры и системы множителей. Структура пространств модулярных и параболических форм в некоторых частных случаях. Приложения к тета-функции. <i>Источники:</i> [Kob], параграфы III.3-III.4, IV.1; [Sar], параграф 1.3; [Iw], параграф 2.8.

5.3 Примеры задач для семинаров и самостоятельной работы

Листок задач 1. Евклидовы решётки (темы 1–3)

1. Докажите, что если P – основной параллелепипед решётки, то $\bigcup_{z \in L} P_z = \mathbb{R}^n$, где P_z – сдвиги P на вектора из L .
2. Докажите, что если $L(B)$ – полная решётка ранга n с базисом $B = (b_i)_{i=1}^n$, $B^* = (b_i^*)_{i=1}^n$ – ортогонализация Грама-Шмидта, то $\text{vol}(L) = \prod_{i=1}^n \|b_i^*\|$. Докажите также, что в общем случае, $\text{vol}(L) = \sqrt{\det(B^T B)}$.
3. Пусть $L = L(B)$ – решётка, L^* – её двойственная, докажите свойства:
 - (a) $L^* = L(B(B^T B)^{-1})$;
 - (b) $(cL)^* = c^{-1}L^*$;
 - (c) $(L^*)^* = L$;
 - (d) $\text{vol}(L^*) = (\text{vol}(L))^{-1}$.
4. Докажите, что все последовательные минимумы решётки $L \subset \mathbb{R}^n$, для которой достигается постоянная Эрмита γ_n , равны между собой.
5. Докажите следующие неравенства: $2r(L) \leq \lambda_1(L) \leq \dots \leq \lambda_n(L) \leq 2R(L) \leq \sqrt{n}\lambda_n(L)$.
6. Докажите теорему Лагранжа о представимости натуральных чисел суммой четырёх квадратов описанным в лекции методом (то есть поиском подходящей решётки).
7. Докажите, что все изображения $x(\alpha) \in \mathbb{R}^n$ элементов поля алгебраических чисел $\alpha \in K$ образуют всюду плотное множество в \mathbb{R}^n .
8. Найдите все единицы поля $\mathbb{Q}(\sqrt{3})$.

9. Докажите, что в поле $\mathbb{Q}(\theta)$, $\theta^3 = 2$, единицы имеют вид $\pm(1 - \theta)^k$.

Листок задач 2. Квадратичные формы (темы 4–7)

1. Докажите, что особенная квадратичная форма всегда представляет 0.
2. Докажите, что если бинарная форма $x^2 - \alpha y^2$ представляет γ_1, γ_2 , то она представляет и $\gamma_1 \gamma_2$.
3. Определите группу Витта для форм над \mathbb{R} и над \mathbb{C} .
4. Найдите какими кольцами \mathbb{Z}_p эквивалентны пары форм: $2x_1x_2$ и $x_1^2 - x_2^2$; $2x_1x_2$ и $x_1^2 + x_2^2$.
5. Докажите, что всякая неособая квадратичная форма над \mathbb{Q}_2 \mathbb{Z}_2 -эквивалентна сумме форм одного из следующих видов: $2^e x^2, 2^e(3x^2), 2^e(5x^2), 2^e(7x^2), 2^e(2x_1x_2), 2^e(2x_1^2 + 2x_1x_2 + 2x_2^2)$.
6. Определите структуру группы Витта над \mathbb{Q} .
7. Найдите число корней $|R_L|$ для решёток $L \in \{A_n, D_n, E_6, E_7, E_8\}$.
8. Докажите что группа Вейля $W(L)$ решётки $L \subset \mathbb{R}^n$ действует неприводимо на \mathbb{R}^n .
9. Докажите что группа Вейля $W(L)$ решётки L действует транзитивно на системе корней R_L .

Листок задач 3. Модулярные формы (темы 8–10)

1. Пусть f – модулярная форма веса k , $g(z) = \frac{1}{2\pi i} f'(z) - \frac{k}{12} E_2(z)f(z)$, докажите, что g – модулярная форма веса $k+2$.
2. Докажите соотношения для рядов Эйзенштейна: $E_4^2 = E_8$, $E_4E_6 = E_{10}$, $E_6E_8 = E_{14}$.
3. Докажите, что E_4 и E_6 алгебраически независимы в пространстве модулярных форм.
4. Докажите, что $E_{12} - E_6^2 = C\Delta$.
5. Докажите, что при $n < 8$ всякая самодвойственная решётка в \mathbb{R}^n изоморфна \mathbb{Z}^n .
6. Пусть $\theta(\chi, z) = \sum_{n=1}^{\infty} \chi(n)e^{-2\pi izn^2}$, найдите функциональное уравнение для $\theta(\chi, z)$.

Листок задач 4. Операторы Гекке и конгруэнц подгруппы (темы 11–12)

1. Докажите, что $\Gamma_1(N)$ является нормальной подгруппой $\Gamma_0(N)$ но не является нормальной в $\Gamma(1)$. Является ли $\Gamma_0(N)$ нормальной в $\Gamma(1)$?
2. Вычислите индексы подгрупп $[\Gamma(1) : \Gamma(N)]$, $[\Gamma_1(1) : \Gamma(N)]$, $[\Gamma_0(1) : \Gamma_1(N)]$, $[\Gamma_0(1) : \Gamma(N)]$, $[\Gamma(1) : \Gamma_0(N)]$.
3. Пусть H – бесконечномерное Гильбертово пространство с базисом (f_n) , T_m – оператор сдвига: $T_m f_n = f_{n+m}$. Докажите, что (T_m) – коммутативное семейство нормальных операторов, при этом у него не существует одновременной собственной функции.
4. Пусть $\alpha \in \mathrm{GL}_2(\mathbb{Q})$ докажите формулу двойного разложения: $\Gamma(1)\alpha\Gamma(1) = \bigcup \Gamma(1)\alpha_i$.
5. Докажите, что $\langle f|\alpha, g \rangle = \langle f, g|\alpha^{-1} \rangle$.

6. Докажите, что $\theta(z)^4 \in M_2(\Gamma_0(4))$, $\eta(4z)^8\eta(2z)^4 \in M_2(\Gamma_0(4))$, а также что эти два элемента линейно независимы.
7. Докажите тождество: $\theta(z) = \eta(2z)^5/(\eta(z)^2\eta(4z)^2)$, $\theta(z) = e^{-\pi i/24}\eta(z+1/2)^2/\eta(2z)$.
8. Опишите пространство $S_{k/2}(\Gamma_0(4))$ и найдите его размерность.

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 экзамену:

1. Евклидовы решётки и подрешётки. Размерность и ранг. Основной параллелепипед. Объем и дискриминант. Унимодулярность и двойственность.
2. Свойства дискретности решёток, теорема Бибербаха.
3. Выпуклость. Теорема Бликфельдта. Лемма Минковского.
4. Приложения леммы Минковского: последовательные минимумы решётки, рациональные приближения.
5. Кольца целых алгебраических чисел. Геометрическое изображение алгебраических чисел и единиц кольца целых алгебраических чисел.
6. Теорема Дирихле о структуре группы единиц кольца целых.
7. Эквивалентность квадратичных форм. Теорема Витта о прямой сумме. Группа Витта.
8. Квадратичный модуль. Целочисленная эквивалентность квадратичных форм. Группа Гротендика.
9. Фундаментальная система корней. Теорема Витта о существовании нормированной фундаментальной системы корней. Диаграммы Коксетера-Дынькина.
10. Приводимые и неприводимые решётки корней, классификация неприводимых решёток, теорема о разложении произвольных решёток корней в прямую сумму неприводимых.
11. Модулярная группа, её действие на верхней комплексной полуплоскости (модель Пуанкаре).
12. Слабомодулярные и модулярные функции. Модулярные и параболические формы. Модулярные функции как функции решёток на комплексной плоскости
13. Нули и полюса модулярных функций. Размерность и структура пространства модулярных форм. Алгебра модулярных форм.

14. Ряды Эйзенштейна, модулярный дискриминант, модулярный инвариант. Разложение рядов Эйзенштейна.
15. Формула суммирования Пуассона. Тета-функция решетки.
16. Свойства унимодулярных решёток. Единственность решетки E_8 . Решётка Ли-ча.
17. Операторы Гекке, коммутативность алгебры операторов Гекке. Действие операторов Гекке на модулярные функции и формы.
18. Скалярное произведение Петерсона. Собственные значения и собственные функции операторов Гекке. Свойства и оценки коэффициентов модулярных форм.
19. Конгруэнц подгруппы полной модулярной группы, фундаментальная область. Модулярные формы для конгруэнц подгрупп
20. Модулярные формы полуцелых весов, тета-функция как модулярная формула полуцелого веса.

Примеры контрольных задач приведены в разделе 5.3.

7 РЕСУРСНОЕ ОБЕСПЕЧЕНИЕ

7.1 Перечень основной и дополнительной литературы

СПИСОК ЛИТЕРАТУРЫ

- [БШ] З.И. Боревич, И.Р. Шафаревич, Теория чисел. Наука, 1972.
- [GM] D. Micciancio, S. Goldwasser, Complexity of Lattice Problems. Springer, 2002.
- [Cass] Дж. Касселс, Рациональные квадратичные формы. Мир, 1982 (J.W.S. Cassels, Rational Quadratic Forms. Academic Press, 1978).
- [Serre] Ж.-П. Серр, Курс арифметики. МИР, 1972 (J.-P. Serre, Cours D'Arithmetique, Presses Universitaire de France, 1970).
- [Eb] W. Ebeling, Lattices and Codes. Springer, 2013.
- [Sar] П. Сарнак, Модулярные формы и их приложения. Фазис, 1998 (P. Sarnak, Some Applications of Modular Forms. Cambridge University Press, 1990).
- [Galb] S.D. Galbraith, Mathematics of Public Key Cryptography. Cambridge University Press, 2012.
- [CS] Дж. Конвей, Н. Слоэн, Упаковки шаров, решётки и группы. Мир, 1990 (J. Conway, N.J.A. Sloane, Sphere Packings, Lattices and Groups. Springer, 1999).

- [Kob] H. Коблиц, Введение в эллиптические кривые и модулярные формы. Мир, 1988 (N. Koblitz, Introduction to Elliptic Curves and Modular Forms. Springer, 1993).
- [Iw] H. Iwaniec, Topics in Classical Automorphic Forms. AMS, 1997.
- [Bump] D. Bump, Automorphic Forms and Representations. Cambridge University Press, 1998.
- [BvdGZ] J.H. Bruinier, G. van der Geer, D. Zagier, The 1-2-3 of Modular Forms. Springer, 2008.
- [DSV] G. Davidoff, P. Sarnak, A. Valette, Elementary Number Theory, Group Theory, and Ramanujan Graphs. Cambridge University Press, 2003.
- [Cox] D.A. Cox, Primes of the Form $x^2 + ny^2$. Wiley, 2013.
- [Micc-LN] Lecture Notes: D. Micciancio, Lattices Algorithms and Applications. 2014-2024.
- [Peik-LN] Lecture Notes: C. Peikert, Lattices in Cryptography. 2022.
- [Reg-LN] Lecture Notes: O. Regev, Lattices in Computer Science. 2004, 2009.
- [Roth-LN] Lecture Notes: T. Rothvoss, Integer Optimization and Lattices. 2016.
- [Schulze-LN] Lecture Notes: R. Schulze-Pillot, Lecture Notes on Quadratic Forms and their Arithmetic. 2020.
- [Clark-LN] P.L. Clark, Quadratic Forms Chapter I: Witt's Theory.
- [Mart] J. Martinet, Perfect Lattices in Euclidean Spaces. Springer, 2003.
- [Gr] R.L. Griess Jr., An Introduction to Groups and Lattices Finite Groups and Positive Definite Rational Lattices. International Press of Boston, 2011.
- [Hat] A. Hatcher, Topology of Numbers. AMS, 2022.

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 требованиям: 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 лекций.

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.