МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Ярославский государственный университет им. П.Г. Демидова»

Кафедра алгебры и математической логики

УТВЕРЖДАЮ

Декан математического факультета

_____ П. Н. Нестеров

«18» мая 2022 г.

Рабочая программа дисциплины

«Теория чисел»

программы подготовки научных и научно-педагогических кадров в аспирантуре

по научной специальности

1.1.5 Математическая логика, алгебра, теория чисел и дискретная математика

Форма обучения очная

Программа одобрена
на заседании кафедры алгебры и математической логики
от «17» мая 2022 года, протокол № 9

Ярославль

1. Цели освоения дисциплины

Целью изучения дисциплины «Теория чисел» является знакомство с основными результатами и методами одной из древнейших и весьма востребованных ныне математических дисциплин. Она лежит в основе всей современной электронной цифровой техники, методах быстрого вычисления математических объектов и моделей самого широкого назначения. Она находит серьезные применения в криптографии и защите информации. Умение свободно обращаться с моделями и методами теории чисел является важным элементом математической грамотности специалиста высокого уровня.

2. Место дисциплины в структуре программы аспирантуры

Дисциплина является дисциплиной по выбору. Данная дисциплина направлена на освоение теории алгебраических и теоретико-числовых структур, их основных методов и идей, имеющих отклик во всей остальной чистой и прикладной математике

3. Планируемые результаты освоения дисциплины: -

В результате освоения дисциплины аспирант должен:
Знать:
Важнейшие теоретико-числовые функции, алгебраические и трансцендентные числа и их рациональные приближения, арифметику алгебраических чисел, теорию полей классов, группу Галуа расширения поля, представления чисел квадратичными формами, проблемы конечности в диофантовой геометрии, дзета-функцию и модулярные формы.

Уметь:
использовать положения теории для решения математических задач в смежных областях, в том числе, с применением вычислительной техники.

Владеть:
навыками анализа основных теоретико-числовых задач и использование техники работы в этой области для получения новых результатов в смежных областях, в том числе, с применением вычислительной техники.

4. Объем, структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 3 зачетные единицы, 108 акад. часов.

№ п/п	Темы (разделы) дисциплины, их содержание	Семестр	Виды учебных занятий и их трудоемкость (в академических часах)	Формы текущего контроля успеваемости

			лекции	практические	лабораторные	консультации	самостоятельная работа	**Форма промежуточной аттестации**
1	Элементарная теория чисел. Сложность арифметических операций. Сравнения. Делимость и алгоритм Евклида. Разложения на простые множители	2	2				10	
2	Важнейшие теоретико-числовые функции. Теоремы Ферма и Эйлера. Сравнения с одним неизвестным.	2	3				10	
3	Сравнения 2-й степени. Символы Лежандра и Якоби. Квадратичный закон взаимности. Разложение действительных чисел в цепные дроби. Алгебраические числа. Рациональные приближения алгебраических чисел.	2	3				10	
4.	Первообразные корни и индексы. Индексы по любому составному модулю. Представления чисел квадратичными формами. Проблемы Ферма и Варинга.	2	3				16	
5	Теорема Лиувилля о приближении алгебраических чисел рациональными дробями. Трансцендентность чисел е и π	2	3				16	
6	Арифметика алгебраических чисел. Теорема Фальтингса и проблемы конечности в диофантовой .геометрии.	2	3				16	
7	Дзета-функция и модулярные формы. Модулярные формы и L-функции.	2	1				10	
						2		Зачет
	Всего 108 час.		**18**			**2**	**18**	

Содержание разделов дисциплины:

1. Элементарная теория чисел. Сложность арифметических операций. Сравнения. Делимость и алгоритм Евклида. Разложения на простые множители
2. Важнейшие теоретико-числовые функции. Теоремы Ферма и Эйлера. Сравнения с одним неизвестным.
3. Сравнения 2-й степени. Символы Лежандра и Якоби. Квадратичный закон взаимности. Разложение действительных чисел в цепные дроби. Алгебраические числа. Рациональные приближения алгебраических чисел.
4. Первообразные корни и индексы. Индексы по любому составному модулю. Представления чисел квадратичными формами. Проблемы Ферма и Варинга.
5. Теорема Лиувилля о приближении алгебраических чисел рациональными дробями. Трансцендентность чисел e и π.
6. Арифметика алгебраических чисел. Теория полей классов. Группа Галуа в арифметических задачах Теорема Фальтингса и проблемы конечности в диофантовой .геометрии.
7. Дзета-функция и модулярные формы. Модулярные формы и L-функции.

5. Образовательные технологии, в том числе технологии электронного обучения и дистанционные образовательные технологии, используемые при осуществлении образовательного процесса по дисциплине

В процессе обучения используются следующие образовательные технологии:

Вводная лекция – дает первое целостное представление о дисциплине и ориентирует студента в системе изучения данной дисциплины. Дается краткий обзор курса, история развития науки и практики, достижения в этой сфере, имена известных ученых, излагаются перспективные направления исследований. На этой лекции высказываются методические и организационные особенности работы в рамках данной дисциплины, а также дается анализ рекомендуемой литературы.

Академическая лекция с элементами лекции-беседы – последовательное изложение материала, осуществляемое преимущественно в виде монолога преподавателя. Элементы лекции-беседы обеспечивают контакт преподавателя с аудиторией, что позволяет привлекать внимание аспирантов к наиболее важным темам дисциплины, активно вовлекать их в учебный процесс, контролировать темп изложения учебного материала в зависимости от уровня его восприятия.

Консультации – вид учебных занятий, являющийся одной из форм контроля самостоятельной работы аспирантов. На консультациях по просьбе аспирантов рассматриваются наиболее сложные разделы дисциплины, преподаватель отвечает на вопросы аспирантов, которые возникают у них в процессе самостоятельной работы.

В процессе обучения используются технологии электронного обучения и дистанционные образовательные технологии:

.

6. Перечень основной и дополнительной литературы, ресурсов информационно-телекоммуникационной сети «Интернет» (при необходимости), рекомендуемых для освоения дисциплины

а) основная литература

1. Боревич З.И., Шафаревич И.Р., Теория чисел. М., Наука, 1985.
2. Виноградов И.М. Основы теории чисел. М., Наука, 1981.

3. Галочкин А.И., Нестеренко Ю.В., Шидловский А.Б. Введение в теорию чисел. М., МГУ, 1995.
4. Манин Ю.И., Панчишкин А.А. Введение в теорию чисел, Итоги науки и техники, Современные проблемы математики, т.49, М. 1990.

б) дополнительная литература

5. Карацуба А.А. Основы аналитической теории чисел. М., Наука, 1983.
6. Кейперс Л., Нидеррейтер Г. Равномерное распределение последовательностей. М., Наука, 1985.
7. Коблиц Н. Курс теории чисел и криптографии, Научное издательство «ТВП», М., 2001
8. Коробков Н.М. Тригонометрические суммы и их приложения. М., Наука, 1989.
9. Сарнак П. Модулярные формы и х приложения, М.: ФАЗИС, 1998
10. Серр Ж.П., Курс арифметики. М., Мир, 1972.
11. Чандрасекхаран К. Введение в аналитическую теорию чисел. М., Мир, 1974.

в) ресурсы сети «Интернет» (при необходимости)

Автоматизированная библиотечно-информационная система «БУКИ-NEXT» http://www.lib.uniyar.ac.ru/opac/bk_cat_find.php

7. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине включает в свой состав следующие помещения:
- учебные аудитории для проведения лекций;
- учебные аудитории для проведения групповых и индивидуальных консультаций,
- учебные аудитории для проведения промежуточной аттестации;
- помещения для самостоятельной работы.

Помещения для самостоятельной работы оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду ЯрГУ.

Автор(ы) :

Заведующий кафедрой алгебры и математической логики
доктор физико-математических наук Л.С. Казарин

Приложение №1 к рабочей программе дисциплины
«Теория чисел»
по научной специальности 1.1.5 Математическая логика, алгебра, теория чисел и дискретная математика

Оценочные материалы
для проведения текущей и/или промежуточной аттестации
аспирантов по дисциплине

1. Контрольные задания и (или) иные материалы, используемые в процессе текущего контроля успеваемости

Задания для самостоятельной работы

1.Написать программу поиска простых чисел на промежутке от 1 до n методом решета Эратосфена. Проверить экспериментально справедливость постулата Бертрана и гипотезы Гольдбаха. Найти количество пар простых чисел-близнецов.

2. Разработать алгоритмы нахождения наибольшего общего делителя целых чисел и коэффициентов Безу с помощью непрерывных дробей и методом Берлекэмпа. Сравнить эффективность алгоритмов.

3. Найти оценку n-го простого числа, опираясь на доказательство Евклида бесконечности множества простых чисел. Доказать бесконечность множества простых чисел вида $4k+3$.

4. Разложение вещественных чисел в непрерывные дроби. Аппроксимация вещественных чисел с помощью непрерывных дробей. Разложения квадратных корней из 2 и из 3.

5. Теоретико-числовые алгоритмы, используемые в криптографии. В частности, теоремы Ферма, Эйлера и символ Лежандра. Быстрое вычисление символа Лежандра.

6.Приближение алгебраических чисел рациональными числами. Существование трансцендентных чисел. Трансцендентность числа e.

7. Характеры конечных абелевых групп. L-функция Дирихле, соответствующая характеру. Связь с дзета - функцией Римана. Теорема Дирихле о бесконечности простых чисел в прогрессии вида $mn+l$ ($n=1,2,\ \ldots$), где m и l взаимно просты.

8.Теорема Чебышева о плотности простых чисел.

9.Нахождение корня квадратного из натурального числа a по модулю p.

10. Проблема Варинга. Представление натуральных чисел в виде степеней целых чисел.

2. Список вопросов и (или) заданий для проведения промежуточной аттестации

Зачет по дисциплине проводится устно по билетам. Каждый билет содержит один теоретический вопрос и одну задачу.

На подготовку к ответу дается 60 минут.

Список вопросов к экзамену:

Список вопросов к зачету:

1. Квадратичный закон взаимности .
2. Первообразные корни и индексы.
3. Неравенства Чебышева для функции $\pi(x)$.
4. Дзета-функция Римана. Асимптотический закон распределения простых чисел.
5. Характеры и L-функции. Теорема Дирихле о простых числах в арифметической прогрессии.
6. Тригонометрические суммы. Модуль гауссовой суммы. Полные тригонометрические суммы и число решений сравнений.
7. Модулярная группа и модулярные функции. Теорема о строении алгебры модулярных форм.
8. Представление целых чисел унимодулярными квадратичными формами.
9. Приближение вещественных чисел рациональными дробями. Теорема Лиувилля о приближении алгебраических чисел рациональными дробями. Примеры трансцендентных чисел.
10. Трансцендентность чисел e и π.

Задачи для зачета

1. Найти мощность множества всех алгебраических чисел.
2. Доказать с помощью неравенства Чебышева постулат Бертрана.
3. Пусть p – нечетное простое число и a – первообразный корень по модулю p^2. Докажите, что a – первообразный корень по модулю p^k для любого $k>2$.
4. Докажите, что нечетное натуральное число n является простым тогда и только тогда, когда оно единственным образом представляется в виде разности квадратов целых неотрицательных чисел.
5. Найти основные единицы в полях $Q((19)^{1/2})$ и $Q((37)^{1/2})$.
6. Какие простые числа представляются формами x^2+5y^2 и $2x^2+2xy+3y^2$?
7. Показать, что для алгебраически замкнутых полей показателей не существует.
8. Определить группу классов Витта для квадратичных форм над полем вещественных чисел и над полем комплексных чисел.
9. Изложить примеры субэкспоненциальных алгоритмов факторизации натуральных чисел.

2.1 Описание процедуры выставления оценки

По итогам экзамена выставляется одна из оценок: «отлично», «хорошо», «удовлетворительно» или «неудовлетворительно».

Оценка «Отлично» выставляется аспиранту, который демонстрирует глубокое и полное владение содержанием материала и понятийным аппаратом дисциплины; осуществляет межпредметные связи; умеет связывать теорию с практикой. Аспирант дает развернутые, полные и четкие ответы на вопросы экзаменационного билета и дополнительные вопросы, соблюдает логическую последовательность при изложении материала. Грамотно использует научную терминологию.

Оценка «Хорошо» выставляется аспиранту, ответ которого на экзамене в целом соответствуют указанным выше критериям, но отличается меньшей обстоятельностью, глубиной, обоснованностью и полнотой. В ответе имеют место отдельные неточности (несущественные ошибки), которые исправляются аспирантом после дополнительных и (или) уточняющих вопросов экзаменатора.

Оценка «Удовлетворительно» выставляется аспиранту, который дает недостаточно полные и последовательные ответы на вопросы экзаменационного билета и дополнительные вопросы, но при этом демонстрирует умение выделить существенные и несущественные признаки и установить причинно-следственные связи. При ответах аспирант допускает ошибки в определении и раскрытии отдельных понятий, формулировке положений, которые аспирант затрудняется исправить самостоятельно. При аргументации ответа аспирант не обосновывает свои суждения. На часть дополнительных вопросов студент затрудняется дать ответ или дает неверные ответы.

Оценка «Неудовлетворительно» выставляется аспиранту, который демонстрирует разрозненные, бессистемные знания; беспорядочно и неуверенно излагает материал; не умеет выделять главное и второстепенное, не умеет соединять теоретические положения с практикой, не устанавливает межпредметные связи; допускает грубые ошибки при определении сущности раскрываемых понятий, явлений, вследствие непонимания их существенных и несущественных признаков и связей; дает неполные ответы, логика и последовательность изложения которых имеют существенные и принципиальные нарушения, в ответах отсутствуют выводы. Дополнительные и уточняющие вопросы экзаменатора не приводят к коррекции ответов аспиранта.

Оценка «Неудовлетворительно» выставляется также аспиранту, который взял экзаменационный билет, но отвечать отказался.