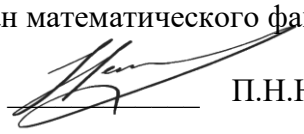
МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Ярославский государственный университет им. П.Г. Демидова

Кафедра алгебры и математической логики

УТВЕРЖДАЮ

Декан математического факультета



П.Н.Нестеров

«18» мая 2021 г.

Рабочая программа дисциплины
«Теория чисел»

Направление подготовки
01.06.01 Математика и механика

Направленность (профиль)
«Математическая логика, алгебра и теория чисел»

Форма обучения очная

Программа рассмотрена
на заседании кафедры алгебры и математической логики
от «16» апреля 2021 года, протокол № 8

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 «Теория чисел» является дисциплиной по выбору вариативной части. 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 обучения по дисциплине – знания, умения, навыки и (или) опыт деятельности, характеризующие этапы формирования компетенций и обеспечивающие достижение планируемых результатов освоения программы аспирантуры, и критерии их оценивания

Процесс изучения дисциплины направлен на формирование следующих компетенций:

Профессиональные компетенции:

- готовность к исследованию в области теории алгебраических структур (полугрупп, групп, колец, полей, модулей и т. д.) (ПК-1);

Код компетенции	Планируемые результаты обучения	Критерии оценивания результатов обучения		
		Пороговый уровень	Продвинутый уровень	Высокий уровень
ПК-1	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	Фрагментарные (неполные) представления об основных теоретико-числовых функциях, алгебраических и трансцендентных числа и их рациональных приближения, арифметику алгебраических чисел, теорию полей классов, группу Галуа расширения поля, представления чисел квадратичными формами, проблемы конечности в диофантовой геометрии, дзета-	Сформированные, но имеющие отдельные пробелы, представления об основных теоретико-числовых функциях, 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	Сформированные, представления об основных теоретико-числовых функциях, алгебраических и трансцендентных числах и их рациональных приближения, арифметику алгебраических чисел, теорию полей классов, группу Галуа расширения поля, представления чисел квадратичными формами, проблемы конечности в

	УМЕТЬ: использовать положения теории для решения математических задач в смежных областях, в том числе, с применением вычислительной техники	В целом успешное, но не систематическое использование положений теории для решения математических задач в смежных областях, в том числе, с применением вычислительной техники	В целом успешное, но содержащее отдельные пробелы использование теории для решения математических задач в смежных областях, в том числе, с применением вычислительной техники	Сформированное умение 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	В целом успешное, но не систематическое применение навыков 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	В целом успешное, но содержащее отдельные пробелы применение навыков 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	Успешное и систематическое применение навыков анализа основных теоретико-числовых задач и использование техники работы в этой области для получения новых результатов в смежных областях в том числе, с применением компьютера

4. Объем, структура и содержание дисциплины

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

Дисциплина изучается в течение второго семестра. Формой итоговой аттестации по дисциплине является зачет.

№ п/п	**Темы (разделы) дисциплины, их содержание**	**Семестр**	**Виды учебных занятий и их трудоемкость (в академических часах)**					**Формы текущего контроля успеваемости** **Форма промежуточной аттестации** ***(по семестрам)***
			лекции	практические	лабораторные	консультации	самостоятельная работа	
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	2	3				10	

	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.	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 e и π	2	3				16	
6	Арифметика алгебраических чисел. Теория полей классов. Группа Галуа в арифметических задачах 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		**18**			**2**	**88**	

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, используемые при осуществлении образовательного процесса по дисциплине

Академическая лекция (или лекция общего курса) – последовательное изложение материала, осуществляемое преимущественно в виде монолога преподавателя. Требования к академической лекции: современный научный уровень и насыщенная информативность, убедительная аргументация, доступная и понятная речь, четкая структура и логика, наличие ярких примеров, научных доказательств, обоснований, фактов. Академическая лекция, как правило, состоит из трех частей: вступления (введения), изложения и заключения:

- *вступление* (введение) определяет тему, план и цель лекции. Оно призвано заинтересовать и настроить аудиторию, сообщить, в чём заключается предмет лекции и (или) её актуальность, основная идея (проблема, центральный вопрос), связь с предыдущими и последующими занятиями, поставить её основные вопросы. Введение должно быть кратким и целенаправленным.
- *изложение* является основной частью лекции, в которой реализуется научное содержание темы, ставятся все узловые вопросы, приводится вся система доказательств с использованием наиболее целесообразных методических приемов. Каждое теоретическое положение должно быть обосновано и доказано, приводимые формулировки и определения должны быть четкими, насыщенными глубоким содержанием.
- *заключение* обобщает в кратких формулировках основные идеи лекции, логически ее завершая. В заключении могут даваться рекомендации о порядке дальнейшего изучения основных вопросов лекции самостоятельно по указанной литературе.

Вводная лекция – дает первое целостное представление о дисциплине (или ее разделе) и ориентирует студента в системе изучения данной дисциплины. Обучающиеся знакомятся с назначением и задачами курса, его ролью и местом в системе учебных дисциплин и в системе подготовки специалиста. 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 курса, а также дается анализ рекомендуемой учебно-методической литературы.

6. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень лицензионного программного обеспечения и информационных справочных систем (при необходимости).

В процессе осуществления образовательного процесса используются:

-- программное обеспечение для создания и демонстрации презентаций, иллюстраций и других учебных материалов:

- Microsoft Windows (в составе Microsoft Imagine Premium Electronic Software Delivery).
- Microsoft OfficeSTD 2013 RUS OLP NL Acdmc 021-10232 Microsoft Open License №0005279522
- MikTeX (свободно распространяемое ПО);

-- для поиска учебной литературы библиотеки ЯрГУ -- Автоматизированная библиотечная информационная система "БУКИ - NEXT" (АБИС "БУКИ - NEXT""БУКИ - NEXT").

-- для работы с алгебраическими структурами используется система алгоритмов GAP, имеющаяся в свободном доступе в Интернете.

7. Перечень основной и дополнительной учебной литературы, необходимых 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»

1. Электронная библиотека учебных материалов ЯрГУ
2. Электронная библиотека ЯрГУ: http://www.lib.uniyar.ac.ru/
3. http://mech.math.msu.su/department/

(**http://www.lib.uniyar.ac.ru/opac/bk_cat_find.php**).

4. Информационная система "Единое окно доступа к образовательным ресурсам" (http://www.edu.ru раздел Учебно-методическая библиотека) или по прямой ссылке (http://www.edu.ru/library).
5. Электронно-библиотечная система "Университетская библиотека online" (www.biblioclub.ru).
6. http:// www.tc26.ru
7. http:// www.nist.gov/manuscript-publicftion-search.cfm?pub_id=919061
6. http://habrahabr.ru/post/210684/
8. http://www.nist.gov/customcf/get pdf.cfm?pub id=919061
9. http://www.streebog.info/news/opredeleny-pobediteli-konkursa-po issledovaniyu-khesh-funksii-stribog/

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

Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине включает в свой состав специальные помещения:
-учебные аудитории для проведения занятий лекционного типа; групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации;

-помещения для самостоятельной работы;
-помещения для хранения и профилактического обслуживания оборудования.

Специальные помещения укомплектованы специализированной мебелью и техническими средствами обучения, служащими для представления информации большой аудитории.

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

Число посадочных мест в лекционной аудитории больше либо равно списочному составу потока, а в аудитории для практических занятий (семинаров) – списочному составу группы обучающихся.

Автор :
Заведующий кафедрой алгебры и математической логики
профессор, д.ф-м.н. Казарин Л.С

Приложение к №1 рабочей программе дисциплины
«Теория чисел»

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

1. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

1.1 Список вопросов и (или) заданий для проведения промежуточной аттестации

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.

Задания 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.

Приложение № 2 к рабочей программе дисциплины
«Теория чисел»

Методические указания для аспирантов по освоению дисциплины

Учебно-методическое обеспечение самостоятельной работы аспирантов по дисциплине

В качестве учебно-методического обеспечения рекомендуется использовать литературу, указанную в разделе № 7 данной рабочей программы.

Перечень ресурсов информационно-телекоммуникационной сети «Интернет», рекомендованных к использованию при освоении дисциплины

Электронные ресурсы ЯрГУ (http://lib.uniyar.ac.ru)
1.Библиографические записи всех видов документов, составляющих фонд библиотеки, на русском и иностранных языках и поступивших позже 1995 года:
http://www.lib.uniyar.ac.ru/opac/bk_cat_find.php (в открытом доступе)

2. Электронная библиотека учебных материалов ЯрГУ:
http://www.lib.uniyar.ac.ru/opac/bk_cat_find.php

3. Электронная картотека «Книгообеспеченность»:
http://www.lib.uniyar.ac.ru/opac/bk_bookreq_find.php

4. Электронно-библиотечная система «Университетская библиотека Online»:
www.biblioclub.ru

5. Проект МАРС: http://mars.arbicon.ru.

6. Электронно-библиотечная система «Лань: http://e.lanbook.com/

7. Научная электронная библиотека eLIBRARY.ru: http://elibrary.ru

8. Англоязычные библиотеки в сети университета:
а) MathSciNet: http://www.ams.org/snhtml/annser.csv - с платформы издателя
http://search.ebscohost.com/ - с платформы Ebscohost
б) Web of Science: http://webofscience.com
в) Scopus: http://www.scopus.com
г) Science The American Association for the Advancement of Science:
http://www.sciencemag.org
д) Ресурсы Springer
SpringerJournals: http://link.springer.com/
SpringerProtocols: http://www.springerprotocols.com/
SpringerMaterials: http://materials.springer.com/
SpringerReference: http://link.springer.com
zbMATH: http://zbmath.org/