

МИНОБРНАУКИ РОССИИ
Ярославский государственный университет им. П.Г. Демидова

Кафедра алгебры и математической логики

УТВЕРЖДАЮ

Декан математического факультета



Нестеров П.Н.

20 июня 2023 г.

Рабочая программа дисциплины

Теория чисел

Направление подготовки (специальности)
02.03.01 Математика и компьютерные науки

Направленность (профиль)
«Программирование, алгоритмы и анализ данных»

Форма обучения очная

Программа рассмотрена
на заседании кафедры
от 18 апреля 2023 г., протокол № 8

Программа одобрена НМК
математического факультета
протокол № 9 от 3 мая 2023 г.

1. Цели освоения дисциплины

Целями освоения дисциплины (модуля) теория чисел являются: обеспечение фундаментальной подготовки в одной из основных областей современной математики, освоение языка и методов одного из наиболее традиционных разделов современной математики, лежащего в основе большей части математики, имеющего разнообразные применения в современной технике и во всей математике

2. Место дисциплины в структуре ООП бакалавриата

Дисциплина является базовой дисциплиной Б1.О.06.01.03 и имеет разносторонние связи со всеми специальными и основными математическими дисциплинами. Полученные при её изучении знания используются в различных специальных курсах, где она зачастую выступает в качестве основы курса. Основные приложения дисциплины таковы:

1. Теория кодирования и её связь с задачами защиты информации.
2. Быстрые вычисления.
3. Теория автоматов.
4. Алгебраические основы криптографии

Она обеспечивает приобретение знаний в соответствии с требованиями Государственных образовательных стандартов, содействует фундаментализации математического образования, формированию научного мировоззрения, логического мышления.

Основная задача дисциплины –

- научить студентов пониманию языка теории чисел, ее логики, умениям применять теорию чисел;
- дать теоретическое обоснование основным теоретико-числовым положениям;
- выработать навыки решения арифметических задач, относящихся к теории делимости целых чисел, методу сравнений и систем сравнений с неизвестной, использование разложений на простые множители, числовым функциям и непрерывным дробям.

Содержание курса реализует поставленные цели и задачи. Материал, изучаемый в курсе, имеет целью освоение фундаментальных алгебраических понятий и выработку навыков в решении теоретико-числовых задач. Практические занятия тесно связаны с теоретическим материалом и опираются на него.

Отбор содержания производится с учетом того, что многие основные сведения из курса алгебры должны быть уже знакомы студентам из курсов “Алгебра”, “Избранные вопросы алгебры”.

3. Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения ООП специалитета

Процесс изучения дисциплины направлен на формирование элементов следующих компетенций в соответствии с ФГОС ВПО по данному направлению:

а) общекультурных (ОК):

способностью логически верно, аргументировано и ясно строить устную и письменную речь на русском языке, готовить и редактировать тексты профессионального назначения, публично представлять собственные и известные научные результаты, вести дискуссии (ОК-7);

способностью к логически-правильному мышлению, обобщению, анализу, критическому осмыслению информации, систематизации, прогнозированию, постановке исследовательских задач и выбору путей их решения на основании принципов научного познания (ОК-9);

б) профессиональных (ПК) и общепрофессиональных (ОПК):

способность применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности (ОПК-2);
способность использовать необходимые математические методы для решения задач профессиональной деятельности;(ОПК-3)

В результате освоения дисциплины обучающийся должен:

знать: основные теоремы теории чисел;

свойства простых чисел, их распределение в ряду натуральных чисел;

методы решения сравнений по модулю натурального числа и арифметические применения теории сравнений;

решение сравнений с помощью непрерывных дробей;

основные теоретико-числовые функции (Эйлера, Мебиуса, Лежандра и Якоби);

методы приближения действительных чисел с помощью цепных дробей.

уметь: решать задачи с помощью методов теории сравнений;

находить значения теоретико-числовых функций;

находить значения наибольшего общего делителя и наименьшего общего кратного с помощью расширенного алгоритма Евклида;

сводить решение сравнений по составному модулю к случаю простого модуля;

применять Китайскую Теорему об Остатках к рационализации вычислений.

владеть математическим аппаратом теории чисел;

методами доказательств утверждений в этой области;

основными алгоритмами теории чисел;

навыками исследования основных моделей теории чисел.

иметь представление:

о значении теории чисел, её месте в системе математического знания, роли в решении прикладных задач;

об истории развития теории чисел и её современных направлениях исследований и открытых проблемах;

- о роли российских и советских математиков в развитии теории чисел;
- об основных проблемах теории чисел и их происхождении;
- о доказательстве Великой Теоремы Ферма;
- о бесконечности множества простых чисел в арифметической прогрессии.

Процесс изучения дисциплины направлен на формирование следующих элементов компетенций в соответствии с ФГОС ВО, ОП ВО и приобретения следующих знаний, умений, навыков и (или) опыта деятельности:

Формируемая компетенция (код и формулировка)	Индикатор достижения компетенции (код и формулировка)	Перечень планируемых результатов обучения
Универсальные компетенции		
УК-1 Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	ИД-1 Знает метод системного анализа, способы обоснования решения (индукция, дедукция, по аналогии) проблемной ситуации.	1. Знать: Основные алгебраические модели и конструкции. 2. Уметь решать алгебраические задачи в конечных и бесконечных алгебрах 3. Владеть навыками вычислений в основных алгебраических системах
Общепрофессиональные компетенции		
ОПК-2 Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности;	ИД-1 Знает основные компоненты системного программного обеспечения; типы операционных систем; командный и программный интерфейс пользователя с операционной системой; типы, организацию	1. Знать: Основные методы и формулировки результатов, использующихся в защите информации 2. Уметь обосновывать алгоритмы защиты информации 3. Владеть навыками быстрых вычислений в основных алгебраических системах
ОПК-3 Способен использовать необходимые математические методы для решения задач профессиональной деятельности;	ИД-1 Знает основные задачи векторной алгебры и аналитической геометрии; возможности координатного метода для исследования различных	1. Знать: Основные математические модели и конструкции. 2. Уметь использовать алгебраические и теоретико-числовые методы для решения профессиональных задач. 3. Владеть навыками вычислений в основных алгебраических системах

4. Структура и содержание дисциплины Теория чисел

Общая трудоемкость дисциплины составляет 2 зачетных единиц, 72 акад. часов.

№ п/п	Темы (разделы) дисциплины, их содержание	Семестр	Виды учебных занятий, включая самостоятельную работу студентов, и их трудоемкость (в академических часах)						Формы текущего контроля успеваемости Форма промежуточной аттестации (по семестрам)
			Контактная работа						
			лекции	практические	лабораторные	консультации	аттестационные испытания	самостоятельная работа	
1.	Предмет и методы теории чисел. Краткий исторический очерк. Влияние теории чисел на развитие других разделов математики. Роль русских и советских математиков в развитии теории чисел	6	1	2				1	
2	.Аксиоматика теории чисел. Метод математической индукции. Бином Ньютона и треугольник Паскаля. Ранняя теория чисел.	6	1	2				1	
3.	Теория делимости целых чисел. Алгоритм деления. Простые числа. Решето Эратосфена. Теорема Евклида о бесконечности множества простых чисел. Основная теорема арифметики и ее следствия. Наибольший общий делитель и наименьшее общее кратное. Основная теорема арифметики. Коэффициенты Безу. Кольцо Гауссовых целых чисел. Расширенный алгоритм Евклида. Связь алгоритма Евклида с непрерывными дробями..	6	2	4		2		2	

4.	Цепные дроби. Подходящие цепные дроби и их свойства. Приближение действительных чисел рациональными. Признак иррациональности числа. Иррациональность числа e . Теорема Лагранжа о разложении квадратичных иррациональностей в цепную дробь. Алгебраические и трансцендентные числа. Существование трансцендентных чисел.	6	2	4			2	
5.	Распределение простых чисел в натуральном ряду. Теорема Чебышева. Ослабленная форма теоремы Чебышева. Понятие о дзета-функции. Гипотеза Римана. Постулат Бертрана	5	2	4			2.7	Контрольная работа 1.
6.	Распределение простых чисел в арифметических прогрессиях Теорема Дирихле. Гипотеза Гольдбаха. Аддитивные задачи теории чисел. Теоремы Линника и Виноградова. Некоторые открытые проблемы	5	2	4		2	2	
7.	Вычеты и классы вычетов по модулю. Полная система вычетов. Приведенная система вычетов. Равносильные сравнения. Арифметические приложения. Признаки делимости чисел на простые числа. Линейные сравнения. Теорема о существовании решений. Простейшие приемы	5	2	4			2	

	решений. Решения сравнений с помощью цепных дробей. Системы сравнений и их решения. Сравнения n-ой степени. Теоремы о решении систем сравнений n-ой степени. Сравнения по составному модулю и их сведение к системе сравнений по простому модулю. Теорема о числе решений сравнения.								
8.	Теоремы Ферма и Эйлера и их следствия. Теорема Вильсона. Разложение числа $n!$ на простые множители. Проблема определения простоты числа. Тест Ферма. Вероятностные алгоритмы. Индикатор Кармайкла источники и каналы.	6	2	4		1		3	Контрольная работа 2.
9	Первообразные корни и индексы. Первообразные корни по модулям p^a и $2p^a$. Разыскание первообразных корней по модулям p^a и $2p^a$. Индексы по модулям p^a и $2p^a$. Таблицы индексов. Индексы по модулю 2^a . Индексы по любому модулю	6	2	4			0.3	2	
							0,3	17,7	зачет
	Всего 72 час		16	32		6	0,3	17,7	

4.Содержание разделов дисциплины

1.Введение. Предмет и методы современной прикладной алгебры. Некоторые проблемы. Краткий исторический очерк. Место прикладной алгебры в системе математического знания и взаимодействие «чистой» и «прикладной» математики. Алгебра и алгоритмика.

2. **Аксиоматика теории чисел.** Метод математической индукции. Бином Ньютона и треугольник Паскаля. Ранняя теория чисел..

3. **Теория делимости целых чисел.**

Алгоритм деления. Простые числа. Решето Эратосфена. Теорема Евклида о бесконечности множества простых чисел. Основная теорема арифметики и ее следствия. Наибольший общий делитель и наименьшее общее кратное. Основная теорема арифметики. Коэффициенты Безу. Кольцо Гауссовых целых чисел. Расширенный алгоритм Евклида. Связь алгоритма Евклида с непрерывными дробями..одного события.

4. **Цепные дроби.** Подходящие цепные дроби и их свойства. Приближение действительных чисел рациональными. Признак иррациональности числа. Иррациональность числа e . Теорема Лагранжа о разложении квадратичных иррациональностей в цепную дробь. Алгебраические и трансцендентные числа. Существование трансцендентных чисел.
5. **Распределение простых чисел в натуральном ряду.** Теорема Чебышева. Ослабленная форма теоремы Чебышева. Понятие о дзета-функции. Гипотеза Римана. Постулат Бертрана
6. **Распределение простых чисел в арифметических прогрессиях** Теорема Дирихле. Гипотеза Гольдбаха. Аддитивные задачи теории чисел. Теоремы Линника и Виноградова. Некоторые открытые проблемы
7. **Вычеты и классы вычетов по модулю.** Полная система вычетов. Приведенная система вычетов. Равносильные сравнения. Арифметические приложения. Признаки делимости чисел на простые числа. Линейные сравнения. Теорема о существовании решений. Простейшие приемы решений. Решения сравнений с помощью цепных дробей. Системы сравнений и их решения. Сравнения n -ой степени. Теоремы о решении систем сравнений n -ой степени. Сравнения по составному модулю и их сведение к системе сравнений по простому модулю. Теорема о числе решений сравнения.
8. **Теоремы Ферма и Эйлера и их следствия.** Теорема Вильсона. Разложение числа $n!$ на простые множители. Проблема определения простоты числа. Тест Ферма. Вероятностные алгоритмы. Индикатор Кармайкла.
9. **Первообразные корни и индексы.** Первообразные корни по модулям p^a и $2p^a$. Разыскание первообразных корней по модулям p^a и $2p^a$. Индексы по модулям p^a и $2p^a$. Таблицы индексов. Индексы по модулю 2^a . Индексы по любому модулю

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. Студенты 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.

Практическое занятие – занятие, посвященное освоению конкретных умений и навыков и закреплению полученных на лекции знаний по предложенному алгоритму.

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:

-- для формирования текстов материалов для промежуточной и текущей аттестации -- программа Microsoft Office, издательская система La Tex (Ams Tex);

7. Перечень современных профессиональных баз данных и информационных справочных систем, используемых при осуществлении образовательного процесса по дисциплине (при необходимости)

В процессе осуществления образовательного процесса по дисциплине используются:

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

8. Перечень основной и дополнительной учебной литературы, ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

а) основная литература:

1. Виноградов И.М. Основы теории чисел: [Электронный ресурс: учебное пособие /И.М.Виноградов – электрон. дан. - Санкт – Петербург: Лань, 2009 – 176 с.
2. Бухштаб А.А. Теория чисел: учебное пособие для вузов. - М.: Лань, 2015.-384с

б) дополнительная литература:

1.Герман О.Н.. Теоретико-числовые методы в криптографии/ О.Н.Герман, Ю.В.Нестеренко -- М: Изд. Центр «Академия», 2012. 271 с.

2.Казарин Л.С., Шалашов В.К. Теория чисел. Часть 1: учебное пособие для вузов. - Ярославль.: ЯрГУ, 2003.-76с.

3.Казарин Л.Г., Шалашов В.К. Теория чисел. Часть 2: учебное пособие для вузов. - Ярославль.: ЯрГУ, 2004.-108с.

ресурсы сети «Интернет»

Электронная библиотека учебных материалов ЯрГУ

1. Электронная библиотека ЯрГУ: <http://www.lib.uniyl.ac.ru/>
2. <http://mech.math.msu.su/departments/>

(http://www.lib.uniyl.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](http://www.tc26.ru)
7. [http:// www.nist.gov/manuscript-publication-search.cfm?pub_id=919061](http://www.nist.gov/manuscript-publication-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/>

9. 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 и практических занятий (семинаров);
- учебные аудитории для проведения групповых и индивидуальных консультаций,
- учебные аудитории для проведения текущего контроля и промежуточной аттестации;
- помещения для самостоятельной работы;
- помещения для хранения и профилактического обслуживания технических средств обучения.

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(ы) :

зав.кафедрой алгебры и математической логики ЯрГУ, д-ф.м.н, профессор Казарин Л.С.

Приложение №1 к рабочей программе
«Теория чисел»

Фонд оценочных средств
для проведения текущей и промежуточной аттестации студентов
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 Контрольные задания и иные материалы,
используемые в процессе текущей аттестации

Задание по теме Аксиоматика теории чисел..

По книге: Виноградов И.М. Основы теории чисел:

Задание по теме Теория делимости целых чисел.

По книге: Виноградов И.М. Основы теории чисел:

По книге Бухштаб А.А. Теория чисел

Задание по теме Цепные дроби. Подходящие цепные дроби и их свойства. Приближение действительных чисел рациональными. Признак иррациональности числа. Иррациональность числа e . Теорема Лагранжа о разложении квадратичных иррациональностей в цепную дробь. Алгебраические и трансцендентные числа. Существование трансцендентных чисел.

По книге: Виноградов И.М. Основы теории чисел:

По книге: Бухштаб А.А. Теория чисел

Задание по теме Распределение простых чисел в натуральном ряду. Теорема Чебышева. Ослабленная форма теоремы Чебышева. Понятие о дзета-функции. Гипотеза Римана. Постулат Бертрана

По книге: Виноградов И.М. Основы теории чисел:

По книге: Бухштаб А.А. Теория чисел

Задание по теме Распределение простых чисел в арифметических прогрессиях
Теорема Дирихле. Гипотеза Гольдбаха. Аддитивные задачи теории чисел. Теоремы Линника и Виноградова. Некоторые открытые проблемы

По книге: Виноградов И.М. Основы теории чисел:
По книге: Бухштаб А.А. Теория чисел

Задание по теме Вычеты и классы вычетов по модулю. Полная система вычетов. Приведенная система вычетов. Равносильные сравнения. Арифметические приложения. Признаки делимости чисел на простые числа. Линейные сравнения. Теорема о существовании решений. Простейшие приемы решений. Решения сравнений с помощью цепных дробей. Системы сравнений и их решения. Сравнения n -ой степени. Теоремы о решении систем сравнений n -ой степени. Сравнения по составному модулю и их сведение к системе сравнений по простому модулю. Теорема о числе решений сравнения.

По книге: Виноградов И.М. Основы теории чисел:
По книге: Бухштаб А.А. Теория чисел

Задание по теме Теоремы Ферма и Эйлера и их следствия. Теорема Вильсона. Разложение числа $n!$ на простые множители. Проблема определения простоты числа. Тест Ферма. Вероятностные алгоритмы. Индикатор Кармайкла

По книге: Виноградов И.М. Основы теории чисел:
По книге: Бухштаб А.А. Теория чисел

Задание по теме Первообразные корни и индексы. Первообразные корни по модулям p^a и $2p^a$. Разыскание первообразных корней по модулям p^a и $2p^a$. Индексы по модулям p^a и $2p^a$. Таблицы индексов. Индексы по модулю 2^a . Индексы по любому модулю

По книге: Виноградов И.М. Основы теории чисел:
По книге: Бухштаб А.А. Теория чисел

Некоторые задания для зачетной работы

В семестре студенты решают задачи, предложенные преподавателем. На семинарах предусмотрены две контрольные работы.

Контрольная работа №1

1. Не выполняя деления, выяснить, делится ли число 1010908899 на 7, 11, 13.
2. Доказать, что среди чисел, представимых в виде многочленов n -ой степени одной переменной с целыми коэффициентами содержится бесконечное множество составных.
3. Разложить в непрерывную дробь корень квадратный из числа 2.
4. Найти наибольший общий делитель d чисел a и b и представить его в виде $d=au+bv$, где u и v – целые, воспользовавшись расширенным алгоритмом Евклида (числа a и b задаются преподавателем индивидуально).
5. Написать программу на языке Pascal или C++ нахождения n -го простого числа.

- Даны числа a и b . Требуется найти рациональное число c , находящееся между ними и имеющее наименьший знаменатель.
- Оценить количество простых чисел, находящихся в промежутке от 1 до 10000.

Контрольная работа №2

- Решить уравнение в целых числах $n! + 10n + 3 = k^2$.
- Доказать, что если n – составное число, то при $n > 4$ выполнено $(n-1)!$ делится на n .
- Доказать, что если $\varphi(n)$ делит n , то n свободно от квадратов.
- Доказать, что 33-я степень любого натурального числа a сравнима с a по модулю 4080.
- Написать программу на языке Pascal или C++ проверки простоты заданного числа.
- Найти все Пифагоровы тройки чисел, состоящие из последовательных чисел.
- При измерении удава в попугаях получился остаток в 3 см. При измерении его в кроликах остаток получился 5 см. В мартышках – 2 см. Чему равна длина удава, если длина шага попугая 6 см., длина шага кролика 37 см, а длина шага мартышки – 53 см?

Вопросы к зачету

- Предметы и методы теории чисел. Роль русских и советских математиков в развитии теории чисел.
- Теория делимости целых чисел. Теорема Евклида о бесконечности множества простых чисел.
- Наибольший общий делитель и наименьшее общее кратное. Основная теорема арифметики и ее следствия. Коэффициенты Безу.
- Кольцо Гауссовых целых чисел. Расширенный алгоритм Евклида и его связь с непрерывными дробями.
- Цепные дроби. Приближение действительных чисел рациональными. Иррациональность числа e .
- Теорема Лагранжа о разложении квадратичных иррациональностей в цепную дробь.
- Алгебраические и трансцендентные числа. Существование трансцендентных чисел.
- Распределение простых чисел в натуральном ряду. Теорема Чебышева. Ослабленная форма теоремы Чебышева. Постулат Бертрана.
- Понятие о дзета-функции Римана. Гипотеза Римана.
- Распределение простых чисел в арифметических прогрессиях. Теорема Дирихле. Гипотеза Гольдбаха.
- Аддитивные задачи теории чисел. Теоремы Линника и Виноградова.
- Вычеты и классы вычетов по модулю. Полная система вычетов. Равносильные сравнения. Признаки делимости чисел на простые числа.
- Линейные сравнения. Теорема о существовании решений. Решение сравнений с помощью цепных дробей.
- Системы сравнений и их решения. Сравнения n -ой степени. Теоремы о решении сравнений n -ой степени.
- Сравнения по составному модулю и их сведение к системе сравнений по простому модулю. Теорема о числе решений сравнения.
- Теоремы Ферма и Эйлера и их следствия. Теорема Вильсона. Разложение числа $n!$ на простые множители.
- Проблема определения простоты числа. Тест Ферма. Индикатор Кармайкла. Вероятностные алгоритмы.
- Сумма делителей и число делителей натурального числа.

19. Мультипликативные функции. Функция Эйлера и ее свойства. Функция Мебиуса.
20. Символы Лежандра и Якоби. Квадратичный закон взаимности.
21. Сведение сравнения второй степени к двучленному сравнению. Двучленные сравнения по простому модулю. Двучленные сравнения по составному модулю.
22. Первообразные корни и индексы. Первообразные корни по модулям p^a и $2p^a$. Индексы по модулям p^a и $2p^a$.
23. Таблицы индексов. Индексы по модулю 2^a . Индексы по любому модулю.

2. Перечень компетенций, этапы их формирования, описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкалы оценивания

2.1 Шкала оценивания сформированности компетенций и ее описание

Оценивание уровня сформированности компетенций в процессе освоения дисциплины осуществляется по следующей трехуровневой шкале:

Пороговый уровень - предполагает отражение тех ожидаемых результатов, которые определяют минимальный набор знаний и (или) умений и (или) навыков, полученных студентом в результате освоения дисциплины. Пороговый уровень является обязательным уровнем для студента к моменту завершения им освоения данной дисциплины.

Продвинутый уровень - предполагает способность студента использовать знания, умения, навыки и (или) опыт деятельности, полученные при освоении дисциплины, для решения профессиональных задач. Продвинутый уровень превосходит пороговый уровень по нескольким существенным признакам.

Высокий уровень - предполагает способность студента использовать потенциал интегрированных знаний, умений, навыков и (или) опыта деятельности, полученных при освоении дисциплины, для творческого решения профессиональных задач и самостоятельного поиска новых подходов в их решении путем комбинирования и использования известных способов решения применительно к конкретным условиям. Высокий уровень превосходит пороговый уровень по всем существенным признакам.

2.2 Перечень компетенций, этапы их формирования, описание показателей и критериев оценивания компетенций на различных этапах их формирования

Код компетенции	Форма контроля	Этапы формирования (№ темы (раздела))	Показатели оценивания	Шкала и критерии оценивания компетенций на различных этапах их формирования		
				Пороговый уровень	Продвинутый уровень	Высокий уровень
Общекультурные компетенции						

УК-1			Знать:	Основные понятия и определения	Понятия, определения, формулировки теорем	Все понятия, определения, доказательства основных теорем
			Уметь:	Решать простейшие задачи	Решать задачи среднего уровня	Решать сложные задачи, доказывать теоремы
			Владеть навыками	Владеть навыками	Знать постановки основных задач. Пользоваться алгоритмами решения	Пользоваться методологией и навыками решения широкого круга научных и практических задач
Профессиональные компетенции						
ОПК-2	Зачет	Темы 2-9	Знание основных теорем теории чисел; Умение решать задачи с помощью методов теории сравнений; Владение математическим аппаратом теории чисел;	Знание основных теоремы теории чисел; свойств простых чисел, их распределение в ряду натуральных чисел; методы решения сравнений по модулю натурального числа и арифметические применения теории сравнений; решение сравнений с помощью непрерывных дробей; основные теоретико-числовые функции (Эйлера, Мебиуса,	Умение решать задачи с помощью методов теории сравнений; находить значения теоретико-числовых функций; находить значения наибольшего общего делителя и наименьшего общего кратного с помощью расширенного алгоритма Евклида; сводить решение сравнений по составному модулю к случаю простого модуля;	Владение математическим аппаратом теории чисел; методами доказательств утверждений в этой области; основными алгоритмами теории чисел; навыками исследования основных моделей теории чисел.

				Лежандра и Якоби);методы приближения действительны х чисел с помощью цепных дробей; надёжности, помехоустойчивости; линейные рекуррентные последовательности, их применения для конструирования радара и псевдослучайных последовательностей	применять Китайскую Теорему об Остатках к рационализации и вычислений.		
--	--	--	--	--	--	--	--

3. Методические рекомендации преподавателю по процедуре оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Целью процедуры оценивания является определение степени овладения студентом ожидаемыми результатами обучения (знаниями, умениями, навыками и (или) опытом деятельности).

Процедура оценивания степени овладения студентом ожидаемыми результатами обучения осуществляется с помощью методических материалов, представленных в разделе «Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций»

3.1 Критерии оценивания степени овладения знаниями, умениями, навыками и (или) опытом деятельности, определяющие уровни сформированности компетенций

Пороговый уровень (общие характеристики):

- владение основным объемом знаний по программе дисциплины;
- знание основной терминологии данной области знаний, стилистически грамотное, логически правильное изложение ответа на вопросы без существенных ошибок;
- владение инструментарием дисциплины, умение его использовать в решении стандартных (типовых) задач;

- способность самостоятельно применять типовые решения в рамках рабочей программы дисциплины;
- усвоение основной литературы, рекомендованной рабочей программой дисциплины;
- знание базовых теорий, концепций и направлений по изучаемой дисциплине;
- самостоятельная работа на практических и лабораторных занятиях, периодическое участие в групповых обсуждениях, достаточный уровень культуры исполнения заданий.

Продвинутый уровень (общие характеристики):

- достаточно полные и систематизированные знания в объёме программы дисциплины;
- использование основной терминологии данной области знаний, стилистически грамотное, логически правильное изложение ответа на вопросы, умение делать выводы;
- владение инструментарием дисциплины, умение его использовать в решении учебных и профессиональных задач;
- способность самостоятельно решать сложные задачи (проблемы) в рамках рабочей программы дисциплины;
- усвоение основной и дополнительной литературы, рекомендованной рабочей программой дисциплины;
- умение ориентироваться в базовых теориях, концепциях и направлениях по изучаемой дисциплине и давать им сравнительную оценку;
- самостоятельная работа на практических и лабораторных занятиях, участие в групповых обсуждениях, высокий уровень культуры исполнения заданий.

Высокий уровень (общие характеристики):

- систематизированные, глубокие и полные знания по всем разделам дисциплины;
- точное использование терминологии данной области знаний, стилистически грамотное, логически правильное изложение ответа на вопросы, умение делать обоснованные выводы;
- безупречное владение инструментарием дисциплины, умение его использовать в постановке и решении научных и профессиональных задач;
- способность самостоятельно и творчески решать сложные задачи (проблемы) в рамках рабочей программы дисциплины;
- полное и глубокое усвоение основной и дополнительной литературы, рекомендованной рабочей программой дисциплины;
- умение ориентироваться в основных теориях, концепциях и направлениях по изучаемой дисциплине и давать им критическую оценку;
- активная самостоятельная работа на практических и лабораторных занятиях, творческое участие в групповых обсуждениях, высокий уровень культуры исполнения заданий.

3.2 Описание процедуры выставления оценки

В зависимости от уровня сформированности каждой компетенции по окончании освоения дисциплины студенту выставляется оценка («зачтено», «незачтено»), которая определяется рабочей программой дисциплины в соответствии с учебным планом.

Оценка «зачет» выставляется студенту, у которого каждая компетенция (полностью или частично формируемая данной дисциплиной) сформирована не ниже, чем на пороговом уровне.

Оценка «незачтено» выставляется студенту, у которого хотя бы одна компетенция (полностью или частично формируемая данной дисциплиной) сформирована ниже, чем на пороговом уровне.

Приложение №2 к рабочей программе дисциплины

« Теория чисел »

(наименование дисциплины)

Методические указания для студентов по освоению дисциплины

Для успешного усвоения данного курса необходимо знание основного материала курсов «Алгебра» и «Математический анализ».

Курс «Теория чисел» насыщен весьма нетривиальными теоремами и, в то же время требует от слушателя высокой алгоритмической культуры. Инновационность применяемых мною методик заключается в соблюдении следующих принципов.

1. Я отхожу от лекции с линейным изложением материала, стараясь задействовать эвристические соображения, раскрыть подоплеку рассуждений, лежащих в основе излагаемого материала.
2. В любом случае не упускается возможность иллюстрации материала на знакомых примерах, сооружаются мостики для связи с другими дисциплинами.
3. Особо акцентируется алгоритмическая сторона теории. Показывается, что абстрактные рассуждения имеют вполне конкретные эффективные приложения.
4. В каждой лекции отводится от 5 до 10 минут на решение студентами самостоятельных заданий. Это может быть лемма, теорема, иллюстративный пример. Цель – максимально активизировать познавательные способности студентов. При этом достигается не механическое усвоение дисциплины (аккуратное переписывание), а ее усвоение в процессе решения конкретных задач. Как работать с понятиями, культура мышления воспитываются таким образом.
5. Чтение лекций сопровождается организацией семинарских занятий. Здесь удастся наряду с новым теоретическим материалом дать некоторое представление о логике науки и о персоналиях.

Учебно-методическое обеспечение

самостоятельной работы студентов по дисциплине

Для самостоятельного изучения дисциплины студентам рекомендуется следующая литература:

Учебно-методическое и информационное обеспечение дисциплины (модуля)

а) основная литература:

1. Виноградов И.М. Основы теории чисел: [Электронный ресурс: учебное пособие /И.М.Виноградов – электрон. дан. - Санкт – Петербург: Лань, 2009 – 176 с.
2. Бухштаб А.А. Теория чисел: учебное пособие для вузов. - М.: Лань, 2015.-384с

б) дополнительная литература:

1.Герман О.Н.. Теоретико-числовые методы в криптографии/ О.Н.Герман, Ю.В.Нестеренко -- М: Изд. Центр «Академия», 2012. 271 с.

2.Казарин Л.С., Шалашов В.К. Теория чисел. Часть 1: учебное пособие для вузов. - Ярославль.: ЯрГУ, 2003.-76с.

3.Казарин Л.Г., Шалашов В.К. Теория чисел. Часть 2: учебное пособие для вузов. - Ярославль.: ЯрГУ, 2004.-108с.

4. Яблокова С.И. Задачи по алгебраической алгоритмике. Практикум. -- Ярославль, 2016. -- 76 с.