

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
Тобольский педагогический институт им. Д.И.Менделеева (филиал)
Тюменского государственного университета

УТВЕРЖДАЮ

Директор

Шилов С.П.

« 28 » мая 2020 г.



ТЕОРИЯ ЧИСЕЛ

Рабочая программа для обучающихся по направлению подготовки
44.03.05 Педагогическое образование (с двумя профилями подготовки):
Профили: математика; информатика
Форма обучения очная

Мальшева Е.Н., Валицкас А.И. Теория чисел. Рабочая программа для обучающихся по направлению подготовки 44.03.05 Педагогическое образование (с двумя профилями подготовки): математика; информатика, форма обучения очная. Тобольск, 2020.

Рабочая программа дисциплины опубликована на сайте ТюмГУ: Теория чисел [электронный ресурс] / Режим доступа: <https://tobolsk.utmn.ru/sveden/education/#>

- © Тобольский педагогический институт им. Д.И.Менделеева (филиал) Тюменского государственного университета, 2020
- © Мальшева Елена Николаевна, 2020
- © Валицкас Алексей Игоревич, 2020

1. Пояснительная записка

Цель изучения дисциплины «Теория чисел» - формирование у студентов систематизированных знаний в области теории чисел, ее месте и роли в системе математических наук, как основы профессионально-педагогических компетенций учителя.

Задачи:

- развивать математическое мышление обучающихся, познакомить с направлениями развития теории чисел;
- демонстрировать применение теории чисел для решения математических и практических задач;
- показать место научной области в системе математических наук;
- дать научное обоснование разделов школьного курса математики, связанных с изучением элементов теории чисел и использованием ее методов.

1.1. Место дисциплины в структуре образовательной программы

Дисциплина «Теория чисел» относится к обязательным дисциплинам вариативной части блока Б1. Учебным планом предусмотрено изучение данной дисциплины в течение 3 семестра.

Для успешного освоения содержания данной дисциплины необходимо успешное освоение дисциплин Математический анализ (1-2 сем.), Алгебра (1-2 сем.), Геометрия (2 сем.)

Изучение данной дисциплины обеспечивает освоение последующих дисциплин и практик:

- Методика преподавания математики (6-8 сем.)
- Решение олимпиадных задач по математике и информатике (6, 7 сем.)
- Решение задач повышенной сложности по математике и информатике (6, 7 сем.)
- Математическая логика и теория алгоритмов (6 сем.)
- Развивающие задачи по математике и информатике (8 сем.)
- Приложения математики в других науках (8 сем.)
- Подготовка учащихся к итоговой аттестации по математике и информатике (8, 9 сем.)
- Методика профильного обучения математике и информатике (9, 10 сем.)
- Преддипломная практика (10 сем.);
- Выпускная квалификационная работа (10 сем.).

1.2. Компетенции обучающегося, формируемые в результате освоения данной дисциплины

Процесс изучения данной дисциплины направлен на формирование элементов следующих компетенций в соответствии с ФГОС ВО и ОП ВО по данному направлению подготовки:

ОК-3 способность использовать естественнонаучные и математические знания для ориентирования в современном информационном пространстве;

ПК-4 способность использовать возможности образовательной среды для достижения личностных, метапредметных и предметных результатов обучения и обеспечения качества учебно-воспитательного процесса средствами преподаваемых учебных предметов

Код и наименование компетенции	Компонент (знаниевый/функциональный)
ОК-3 способность использовать естественнонаучные и математические	Знает основные понятия и формулы теории чисел: основные теоретико-числовые понятия;

Код и наименование компетенции	Компонент (знаниевый/функциональный)
знания для ориентирования в современном информационном пространстве	основные результаты о делимости целых чисел и теории сравнений; основные алгоритмы решения стандартных задач
	<p>Может использовать теоретические знания для решения математических и прикладных задач:</p> <ul style="list-style-type: none"> • применять теорему о делении с остатком и свойства делимости к решению различных арифметических задач; • применять алгоритм Евклида для нахождения наибольшего общего делителя целых чисел, его линейного разложения и наименьшего общего кратного; • используя “решето” Эратосфена, составлять таблицы простых чисел и решать задачи на применение основной теоремы арифметики и свойств простых чисел. • находить разложение заданного рационального числа в конечную цепную дробь и разложение заданного иррационального числа в бесконечную цепную дробь, вычислять подходящие дроби и применять свойства подходящих дробей при решении задач; • применять определение и свойства сравнений по заданному модулю при составлении полной и приведённой систем вычетов; • вычислять значения функции Эйлера и остатки арифметических выражений от деления на заданное число, используя свойства сравнений и теоремы Эйлера и Ферма. • решать различными способами линейные сравнения первой степени с одним неизвестным. • применять для решения задач алгоритмы нахождения показателя и первообразного корня по заданному модулю. Уметь решать двучленные сравнения, используя таблицы индексов. • применять обобщённый признак делимости Паскаля для конструирования конкретных признаков делимости. • проверять правильность выполнения простейших арифметических действий с помощью сравнений по модулям 9 и 11. • определять по внешнему виду обыкновенной дроби вид её десятичного разложения (конечная десятичная дробь, чисто или смешанно периодическая), уметь находить длины периода и предпериода этого

Код и наименование компетенции	Компонент (знаниевый/функциональный)
	десятичного разложения; • находить аннулирующие уравнения для некоторых простых видов алгебраических чисел.
ПК-4 способность использовать возможности образовательной среды для достижения личностных, метапредметных и предметных результатов обучения и обеспечения качества учебно-воспитательного процесса средствами преподаваемых учебных предметов	Знает место изучения элементов дисциплины в курсе математики основной и старшей школы, их межпредметные связи
	Может доступно объяснить решение задач в области теории чисел, показать область применения знаний

2. Структура и трудоемкость дисциплины

Таблица 1

Вид учебной работы	Всего часов	Часов в семестре
		4
Общая трудоемкость	зач. ед.	2
	час	72
Из них:		
Часы аудиторной работы (всего):	32	32
Лекции	16	16
Практические занятия	16	16
Лабораторные / практические занятия по подгруппам		
Часы внеаудиторной работы, включая самостоятельную работу обучающегося	40	40
Вид промежуточной аттестации (зачет, диф. зачет, экзамен)		зачет

3. Система оценивания

3.1. Текущий контроль

Оценивание результатов освоения дисциплины может осуществляться в рамках балльной системы, разработанной преподавателем и доведенной до сведения обучающихся на первом занятии

№ темы	Формы оцениваемой работы	Количество часов	Макс. количество баллов
4 семестр			
Лекции 1-8	Конспект Контрольные вопросы	16	16
Практические занятия 1-8	Решение задач. Объяснение решения у доски. Контрольная работа	32	48
Самостоятельная работа	Домашние задания. Самостоятельные работы Подготовка к экзамену	40	46
	Итого	72	100

3.2. Промежуточный контроль

Обучающиеся, выполнившие учебный план, получают оценку «зачтено» (4 семестр). Проводится зачет в форме собеседования по теоретическому вопросу и решения примера по теме вопроса.

Промежуточная аттестация может быть выставлена с учетом совокупности баллов, полученных обучающимся в рамках текущего контроля.

Перевод баллов в оценки:

0-60 – не зачтено,

61-100 – зачтено.

4. Содержание дисциплины

4.1. Тематический план дисциплины

Таблица 2

№	Темы	Объем дисциплины, час.				
		Всего	Виды аудиторной работы			Иные виды контактной работы
			Лекции	Практические занятия	Лабораторные / практические занятия по подгруппам	
3 семестр						
1	Теория делимости в кольце целых чисел	18	6	6		
2	Теория сравнений	18	4	4		
3	Арифметические приложения теории сравнений	18	4	4		
4	Алгебраические и трансцендентные числа	18	2	2		
Итого (часов)		72	16	16		

4.2. Содержание дисциплины по темам

4.2.1. Темы лекций

№.	Раздел	Тема лекции
1	Теория делимости в кольце целых чисел	<p><i>Делимость целых чисел</i> Теорема о делении с остатком. Делимость нацело и её свойства. Наибольший общий делитель. Алгоритм Евклида. Линейное разложение <i>НОД</i>. Наименьшее общее кратное. Взаимно простые числа и их свойства.</p> <p><i>Основная теорема арифметики</i> Простые числа и их свойства. Основная теорема арифметики. Описание делителей натурального числа. Количество $\tau(n)$ и сумма $\sigma(n)$ делителей натурального числа. Нахождение <i>НОД</i> и <i>НОК</i> с помощью канонических</p>

№.	Раздел	Тема лекции
		<p>разложений. Бесконечность количества простых чисел в арифметических прогрессиях.* Решето Эратосфена.</p> <p><i>Цепные дроби</i></p> <p>Конечные цепные дроби. Подходящие дроби и их основные свойства. Теорема о представлении рациональных чисел конечными цепными дробями. Применение конечных цепных дробей к нахождению линейного разложения <i>НОД</i>. Бесконечные цепные дроби. Значение бесконечной цепной дроби. Теорема о представлении иррациональных чисел бесконечными цепными дробями. Признак иррациональности числа и иррациональность числа <i>e</i>. Подходящие дроби как наилучшие приближения действительных чисел рациональными.*</p>
2	Теория сравнений	<p>Отношение сравнимости по модулю и его основные свойства. Кольцо Z_n, поле Z_p и группа Z_n^*. Полная и приведённая системы вычетов. Мультипликативные функции. Функция Эйлера и её основные свойства. Теоремы Эйлера и Ферма. Китайская теорема об остатках. Полиномиальные сравнения и их решения. Редукция сравнения по составному модулю к модулю, являющемуся степенью простого числа, а затем – к простому модулю. Структура решений линейного сравнения первой степени. Методы решения. Показатель числа (или класса вычетов) по заданному модулю и его основные свойства. Первообразные корни по заданному модулю. Количество и структура первообразных корней. Существование первообразных корней по простому модулю. Первообразные корни по модулям p и $2p$ (p – простое число). Индекс числа (или класса вычетов) относительно первообразного корня по данному модулю. Индексы по модулям p и $2p$ (p – простое число). Двучленные сравнения по простому модулю. Квадратичные вычеты и невычеты. Символ Лежандра и его свойства. Квадратичный закон взаимности Гаусса*. Сравнения второй степени по произвольному модулю*.</p>
3	Арифметические приложения теории сравнений	<p>Нахождение остатков полиномиальных и экспоненциальных выражений с помощью теоремы Эйлера. Проверка арифметических действий с помощью сравнений по подходящим модулям. Обобщённый признак делимости Паскаля. Признаки делимости на $2^m, 5^m, 3, 9, 11 [7, 13]^*$. Конструирование признаков делимости на заданное число. Конечные и бесконечные десятичные дроби.*</p>
4	Алгебраические и трансцендентные числа	<p>Определение алгебраических и трансцендентных (над Q) чисел. Доказательство существования трансцендентных чисел по Кантору.* Теорема Эрмита-Линдемана.* Теорема Лиувилля о приближениях алгебраического числа рациональными числами и её применение к построению трансцендентных чисел и доказательству иррациональности некоторых чисел.*</p>

4.2.2. Темы практических занятий

раздел	№ работы	Тема	Кол-во часов
1	Практическая работа 1.	Теорема о делении с остатком. Наибольший общий делитель. Алгоритм Евклида. Линейное разложение НОД. Наименьшее общее кратное. Проверка числа на простоту. Каноническое разложение натурального числа	2
	Практическая работа 2.	Вычисление числа $\tau(n)$ и суммы $\sigma(n)$ натуральных делителей. Нахождение НОД и НОК. Конечные цепные дроби. Подходящие дроби Представление рациональных чисел конечными цепными дробями. Применение конечных цепных дробей к нахождению линейного разложения НОД.	2
	Практическая работа 3.	Представление иррациональных чисел бесконечными цепными дробями. Подходящие дроби как наилучшие приближения действительных чисел рациональными.	2
2	Практическая работа 4.	Отношение сравнимости по модулю и его основные свойства. Кольцо Z_n , поле Z_p и группа Z_n^* . Полная и приведённая системы вычетов. Вычисление функции Эйлера. Теоремы Эйлера и Ферма. Структура решений линейного сравнения первой степени. Методы решения.	2
	Практическая работа 5.	Первообразные корни и индексы по заданному модулю Количество и структура первообразных корней. Двучленные сравнения по простому модулю.	2
3	Практическая работа 6.	Нахождение остатков полиномиальных и экспоненциальных выражений с помощью теоремы Эйлера. Проверка арифметических действий с помощью сравнений по подходящим модулям. Обобщённый признак делимости Паскаля. Признаки делимости на 2^t , 5^t , 3 , 9 , 11 [7 , 13]*. Конструирование признаков делимости на заданное число.	2
	Практическая работа 7	Конечные и бесконечные десятичные дроби: длины периодов и предпериодов.	2
4	Практическая работа 8.	Определение алгебраических и трансцендентных (над Q) чисел. Минимальные уравнения алгебраических чисел. Алгебраические действия с алгебраическими числами. Построение трансцендентных чисел Лиувилля.	2

4.2.3. Образцы средств для проведения текущего контроля

Текущий контроль осуществляется проверкой наличия конспектов лекций и собеседования по контрольным вопросам, выполнения практических работ и домашних заданий при самостоятельной работе.

Контрольные вопросы

1. Теорема о делении с остатком. Делимость нацело и её свойства.
2. Наибольший общий делитель.
3. Алгоритм Евклида.

4. Линейное разложение *НОД*.
5. Наименьшее общее кратное.
6. Взаимно простые числа и их свойства.
7. Простые числа и их свойства.
8. Основная теорема арифметики.
9. Описание делителей натурального числа.
10. Количество $\tau(n)$ и сумма $\sigma(n)$ делителей натурального числа.
11. Нахождение *НОД* и *НОК* с помощью канонических разложений.
12. Бесконечность количества простых чисел в арифметических прогрессиях.*
13. Решето Эратосфена.
14. Конечные цепные дроби.
15. Подходящие дроби и их основные свойства.
16. Теорема о представлении рациональных чисел конечными цепными дробями.
17. Применение конечных цепных дробей к нахождению линейного разложения *НОД*.
18. Бесконечные цепные дроби. Значение бесконечной цепной дроби.
19. Теорема о представлении иррациональных чисел бесконечными цепными дробями.
20. Признак иррациональности числа и иррациональность числа e .
21. Подходящие дроби как наилучшие приближения действительных чисел рациональными.*
22. Отношение сравнимости по модулю и его основные свойства.
23. Кольцо Z_n , поле Z_p и группа Z_n^* .
24. Полная и приведённая системы вычетов.
25. Мультипликативные функции.
26. Функция Эйлера и её основные свойства.
27. Теоремы Эйлера и Ферма.
28. Китайская теорема об остатках.
29. Полиномиальные сравнения и их решения.
30. Редукция сравнения по составному модулю к модулю, являющемуся степенью простого числа, а затем – к простому модулю.
31. Структура решений линейного сравнения первой степени. Методы решения.
32. Показатель числа (или класса вычетов) по заданному модулю и его основные свойства.
33. Первообразные корни по заданному модулю. Количество и структура первообразных корней.
34. Существование первообразных корней по простому модулю.
35. Первообразные корни по модулям p и $2p$ (p – простое число).
36. Индекс числа (или класса вычетов) относительно первообразного корня по данному модулю.
37. Индексы по модулям p и $2p$ (p – простое число).
38. Двучленные сравнения по простому модулю.
39. Квадратичные вычеты и невычеты.
40. Символ Лежандра и его свойства.
41. Квадратичный закон взаимности Гаусса*. Сравнения второй степени по произвольному модулю*.
42. Нахождение остатков полиномиальных и экспоненциальных выражений с помощью теоремы Эйлера.
43. Проверка арифметических действий с помощью сравнений по подходящим модулям.
44. Обобщённый признак делимости Паскаля.
45. Признаки делимости на $2^m, 5^m, 3, 9, 11 [, 7, 13]^*$.

46. Конструирование признаков делимости на заданное число.
47. Конечные и бесконечные десятичные дроби.*
48. Определение алгебраических и трансцендентных (над \mathcal{Q}) чисел.
49. Доказательство существования трансцендентных чисел по Кантору.*
50. Теорема Эрмита-Линдемана.*
51. Теорема Лиувилля о приближениях алгебраического числа рациональными числами и её применение к построению трансцендентных чисел и доказательству иррациональности некоторых чисел.*

Практические задания.

1. Укажите частное и остаток от деления ± 520 на ± 23 .
2. Двумя способами найдите $\text{НОК}[134, 126]$ и $\text{НОД}(134, 126)$, вычислите линейное разложение $\text{НОД}(134, 126)$.
3. Докажите, что если $x^2 + y^2 = z^2$, то $x, y \in M_{12}$.
4. При каких $n \in \mathbb{N}$ $2^{2n+1} - 5 \in M_3$?
5. При каких $n \in \mathbb{N}$ $n^3 - 5n + 2 \in M_7$?
6. Разложите $\frac{2121}{1500}$ в конечную цепную дробь и найдите все её подходящие дроби.
7. Найдите каноническое разложение числа $n = 1496$.
8. Найдите число и сумму натуральных делителей числа 1358.
9. Найдите число и сумму целых делителей числа 1358.
10. Докажите, что сумма трёх последовательных натуральных степеней числа 2 делится на 14.
11. С помощью конечных цепных дробей найдите линейное разложение $\text{НОД}(1340, 1260)$.
12. Разложите $\sqrt{5}$ в бесконечную цепную дробь.
13. Найдите первые три цифры разложения в бесконечную цепную дробь числа 2π .

Домашние задания.

Задание 1. Функция $\pi(x)$ и неравенство Чебышева.

1. Что такое простое число?
2. Каково определение функции $\pi(x)$?
3. Вычислите $\pi(0, 5)$, $\pi(2, 999)$, $\pi(17)$.
4. Сформулируйте неравенства Чебышева.
5. Сформулируйте асимптотический закон распределения простых чисел.
6. Сформулируйте постулат Бертрана.

Задание 2. Представление квадратичных иррациональностей периодическими цепными дробями.

1. Что такое бесконечная цепная дробь?
2. Приведите примеры бесконечных цепных дробей.
3. Что такое квадратичная иррациональность?
4. Приведите примеры квадратичных иррациональностей.
5. Что такое (смешанно) периодическая бесконечная цепная дробь?
6. Приведите примеры (смешанно) периодических бесконечных цепных дробей.
7. Сформулируйте теорему Лагранжа.

8. Изложите основные идеи доказательства теоремы Лагранжа.
9. Разложите в бесконечные цепные дроби иррациональности $\sqrt{13}$, $\frac{1+\sqrt{3}}{3}$.
10. Сформулируйте теорему о чисто периодических бесконечных цепных дробях.
11. Сформулируйте теорему о разложении в периодические бесконечные цепные дроби квадратных корней из натуральных неквадратных чисел.
12. Разложите в бесконечные цепные дроби $\sqrt{12}$, $\sqrt{17}$, $\sqrt{19}$.

Задание 3. Представление натуральных чисел в виде суммы двух квадратов.

1. Что такое задача о представлении натуральных чисел в виде суммы двух квадратов?
2. Представьте (если возможно) в виде сумм двух квадратов числа 3, 4, 5, 7, 11, 13, 27.
3. Сформулируйте основной результат о представлении простого числа в виде суммы двух квадратов.
4. Докажите, что простое число вида $p = 4n+3$ не представимо в виде суммы двух квадратов.
5. Изложите основные идеи доказательства представимости простого числа вида $p = 4n+1$ в виде суммы двух квадратов.
6. Сформулируйте общий результат о представлении натурального числа в виде суммы двух квадратов.
7. Докажите, что если два числа представимы в виде суммы двух квадратов, то и их произведение тоже представимо в этом виде.
8. Какова связь задачи о представлении натуральных чисел в виде суммы двух квадратов с теорией разложения квадратичных иррациональностей в цепные дроби?
9. Найдите, основываясь на теории разложения квадратичных иррациональностей в цепные дроби, представление в виде суммы двух квадратов простых чисел $p = 73, 97, 101$.

Задание 4. Приближения действительных чисел подходящими дробями.

1. Что такое подходящие дроби?
2. Приведите примеры подходящих дробей.
3. Сформулируйте основные свойства подходящих дробей.
4. Докажите несколько нетривиальных свойств подходящих дробей.
5. Обоснуйте сходимости подходящих дробей.
6. Найдите приближение числа e подходящими дробями с точностью до 0,001.
7. Сформулируйте и докажите результат о том, что рациональная дробь, достаточно хорошо аппроксимирующая действительное число, совпадает с одной из подходящих дробей.

Задание 5. Системы сравнений.

1. Что такое полиномиальное сравнение?
2. Что такое система полиномиальных сравнений?
3. Что значит решить систему полиномиальных сравнений?
4. Сформулируйте теорему о структуре решений системы сравнений первой степени.
5. Приведите примеры совместной и несовместной систем сравнений первой степени.
6. Докажите что любая система сравнений первой степени эквивалентна системе сравнений с попарно взаимно простыми модулями.
7. Решите системы:

$$\begin{cases} 2 \cdot x \equiv 1 \pmod{6} \\ 3 \cdot x \equiv 2 \pmod{4} \\ 5 \cdot x \equiv 7 \pmod{8} \end{cases}, \begin{cases} 32 \cdot x \equiv 14 \pmod{24} \\ 13 \cdot x \equiv 222 \pmod{144} \\ 15 \cdot x \equiv 77 \pmod{88} \end{cases}, \begin{cases} 32 \cdot x \equiv 14 \pmod{27} \\ 13 \cdot x \equiv 22 \pmod{144} \\ 15 \cdot x \equiv 77 \pmod{88} \end{cases}$$

Задание 6. Квадратичные вычеты и невычеты.

1. Что такое квадратичное сравнение?
2. Что такое квадратичный вычет и невычет?
3. Приведите примеры квадратичных вычетов и невычетов по различным модулям.
4. Докажите, что по любому простому модулю количество квадратичных вычетов равно количеству квадратичных невычетов.
5. Докажите, что решение произвольного квадратичного сравнения $a \cdot x^2 + b \cdot x + c \equiv 0 \pmod{m}$ сводится к решению двучленного сравнения вида $x^2 \equiv A \pmod{M}$.
6. Опишите алгоритм решения сравнения вида $x^2 \equiv A \pmod{M}$ по любому модулю M .
7. Решите квадратичные сравнения:
 $3x^2 + 2x - 5 \equiv 0 \pmod{5}$, $8x^2 - x + 1 \equiv 0 \pmod{12}$.

Задание 7. Символ Лежандра и закон взаимности Гаусса.

1. Что такое символ Лежандра?
2. Какая связь символа Лежандра с квадратичными сравнениями?
3. Сформулируйте основные правила для вычисления символа Лежандра.
4. Докажите несколько нетривиальных правил.
5. Вычислите $\left(\frac{15}{7}\right)$, $\left(\frac{43}{59}\right)$, $\left(\frac{55}{2}\right)$.
6. Сформулируйте квадратичный закон взаимности Гаусса.
7. Как связаны $\left(\frac{43}{59}\right)$ и $\left(\frac{59}{43}\right)$, $\left(\frac{53}{2}\right)$ и $\left(\frac{2}{53}\right)$, $\left(\frac{37}{101}\right)$ и $\left(\frac{101}{37}\right)$?
8. Разрешимы ли сравнения: $x^2 \equiv 17 \pmod{43}$, $x^2 \equiv 43 \pmod{17}$?
9. Опишите основные идеи любимого Вами доказательства квадратичного закона взаимности Гаусса.

Задание 8. Теорема Лиувилля о приближениях алгебраического числа рациональными числами и её применение к построению трансцендентных чисел и доказательству иррациональности некоторых чисел.

2. Что такое алгебраическое число?
3. Что такое трансцендентное число?
4. Докажите, что число $\sqrt[3]{1 + \sqrt{2}}$ является алгебраическим.
5. Приведите известные Вам примеры трансцендентных чисел.
6. Сформулируйте теорему Лиувилля.
7. Докажите теорему Лиувилля для квадратичной иррациональности.
8. Опишите основные идеи общего доказательства теоремы Лиувилля.
9. Приведите пример трансцендентного числа Лиувилля.

5. Учебно-методическое обеспечение и планирование самостоятельной работы обучающихся

№	Темы	Виды СРС
1.	Теория делимости в кольце целых чисел	Выполнение домашних заданий 1-4. Изучение дополнительных вопросов.
2.	Теория сравнений	Выполнение домашних заданий 5-7. Изучение дополнительных вопросов.
3.	Арифметические приложения теории сравнений	Изучение дополнительных вопросов.
4.	Алгебраические и трансцендентные числа	Выполнение домашних заданий 8. Изучение дополнительных вопросов.
5.	Функция $\pi(x)$ и неравенство Чебышева.	Вопросы, выносимые на самостоятельное изучение
6.	Представление квадратичных иррациональностей периодическими цепными дробями.	Вопросы, выносимые на самостоятельное изучение
7.	Представление натуральных чисел в виде суммы двух квадратов.	Вопросы, выносимые на самостоятельное изучение
8.	Приближения действительных чисел подходящими дробями.	Вопросы, выносимые на самостоятельное изучение
9.	Системы сравнений.	Вопросы, выносимые на самостоятельное изучение
10.	Квадратичные вычеты и невычеты.	Вопросы, выносимые на самостоятельное изучение
11.	Символ Лежандра и закон взаимности Гаусса.	Вопросы, выносимые на самостоятельное изучение
12.	Теорема Лиувилля о приближениях алгебраического числа рациональными числами и её применение к построению трансцендентных чисел и доказательству иррациональности некоторых чисел.	Вопросы, выносимые на самостоятельное изучение

6. Промежуточная аттестация по дисциплине (модулю)

6.1. Оценочные материалы для проведения промежуточной аттестации по дисциплине

В 4 семестре зачет проходит в форме собеседования собеседование по 2 вопросам: теоретический вопрос и решение примера по теме вопроса.

Вопросы к экзамену

1. Теорема о делении целых чисел с остатком.
2. Основные свойства делимости целых чисел нацело.
3. *НОД* и *НОК* целых чисел: определение, свойства, способы нахождения, примеры.
4. Алгоритм Евклида и линейное разложение $\text{НОД}(a, b)$.
5. Взаимно простые числа и их свойства. Примеры.
6. Простые числа и их свойства. Основная теорема арифметики.
7. Вычисление $\text{НОД}(a, b)$ и $\text{НОК}[a, b]$ с помощью канонических разложений чисел a, b . Примеры.
8. Функция Эйлера: определение, вычисление $\varphi(p^\alpha)$, примеры.
9. Функция Эйлера: мультипликативность, примеры.
10. Бесконечность множества простых чисел. Решето Эратосфена.
11. Представление рациональных чисел конечными цепными дробями.

12. Подходящие дроби и их основные свойства.
13. Представление иррациональных чисел бесконечными цепными дробями. Примеры.
14. Квадратичные иррациональности и периодические бесконечные цепные дроби. Примеры.
15. Сравнения и их свойства. Проверка арифметических действий с помощью сравнений. Примеры.
16. Кольцо вычетов Z_m , группа Z_m^* , поле Z_p .
17. Общий признак делимости Паскаля. Признаки делимости на $2^n, 5^n, 3, 9, 11$.
18. Теоремы Эйлера и Ферма. Примеры использования для вычисления остатков.
19. Полиномиальные сравнения и их решения. Редукция сравнения по составному модулю к модулю, являющемуся степенью простого числа, а затем – к простому модулю.
20. Теорема о сравнениях первой степени. Различные методы решения сравнений первой степени. Примеры.
21. Показатели и их свойства. Первообразные корни. Нахождение первообразных корней. Примеры.
22. Существование первообразных корней по простому модулю. Примеры.
23. Представление рациональных чисел десятичными дробями. Длина периода десятичного представления рационального числа. Примеры.
24. Индексы и их свойства. Таблицы индексов и антииндексов. Решение двучленных сравнений $ax^n \equiv b \pmod{m}$ с помощью индексов. Примеры.
25. Числа алгебраические и трансцендентные. Теорема Лиувилля и построение трансцендентных чисел. Примеры.

6.2. Критерии оценивания компетенций:

Таблица 4

Карта критериев оценивания компетенций

Код и наименование компетенции	Компонент (знаниевый/функциональный)	Оценочные материалы	Критерии оценивания
ОК-3 способность использовать естественнонаучные и математические знания для ориентирования в современном информационном пространстве	Знает основные понятия и формулы теории чисел: основные теоретико-числовые понятия; основные результаты о делимости целых чисел и теории сравнений; основные алгоритмы решения стандартных задач	Контрольные вопросы. Зачет.	<p><i>Пороговый уровень:</i> может выполнять работы под контролем преподавателя.</p> <p><i>Базовый уровень:</i> может выполнять работы самостоятельно.</p> <p><i>Повышенный уровень:</i> готов выполнять работы в условиях учебно-воспитательного процесса с обучающимися.</p>
	Может использовать теоретические знания для решения математических и прикладных задач	Практические работы Домашние задания. Зачет.	
ПК-4 способность использовать возможности образовательной среды для достижения личностных, метапредметных и предметных результатов	Знает место изучения элементов дисциплины в курсе математики основной и старшей школы, их межпредметные связи	Контрольные вопросы Зачет.	<p><i>Пороговый уровень:</i> может выполнять работы под контролем преподавателя.</p> <p><i>Базовый уровень:</i> может выполнять работы самостоятельно.</p> <p><i>Повышенный уровень:</i></p>
	Может доступно объяснить решение задач в области	Практические работы.	

Код и наименование компетенции	Компонент (знаниевый/функциональный)	Оценочные материалы	Критерии оценивания
обучения и обеспечения качества учебно-воспитательного процесса средствами преподаваемых учебных предметов	теории чисел, показать область применения знаний	Зачет.	готов выполнять работы в условиях учебно-воспитательного процесса с обучающимися.

7. Учебно-методическое и информационное обеспечение дисциплины (модуля)

7.1 Основная литература:

1. Кнауб, Л. В. Теоретико-численные методы в криптографии [Электронный ресурс] : Учеб. пособие / Л. В. Кнауб, Е. А. Новиков, Ю. А. Шитов. - Красноярск : Сибирский федеральный университет, 2011. - 160 с. – URL: <https://new.znaniyum.com/read?id=86549> – Режим доступа: по подписке ТюмГУ.

7.2 Дополнительная литература:

1. Шидловский, А. Б. Диофантовы приближения и трансцендентные числа: учебное пособие / А.Б. Шидловский. - 2-е изд., испр. - Москва : ФИЗМАТЛИТ, 2007. - 272 с. - URL: <https://znaniyum.com/read?id=221947> – Режим доступа: по подписке ТюмГУ.

2. Шуман, Г. И. Алгебра и геометрия : учеб. пособие / Г.И. Шуман, О.А. Волгина, Н.Ю. Голодная. - Москва : РИОР : ИНФРА-М, 2019. — (Высшее образование). - 160 с. – URL: <https://znaniyum.com/read?id=334888> – Режим доступа: по подписке ТюмГУ

7.3 Интернет-ресурсы:

1. Единое окно доступа к информационным ресурсам. – URL: <http://window.edu.ru> Режим доступа: свободный.
2. Портал образования. – URL: <https://portalobrazovaniya.ru> Режим доступа: свободный.
3. Российское образование. Федеральный портал. – URL: <http://www.edu.ru> Режим доступа: свободный.
4. Малая академия наук "Интеллект будущего" – URL: <https://new.future4you.ru>. Режим доступа: свободный.
5. Наука и образование ON-LINE. Школьникам. – URL: <https://eee-science.ru/announcements-events/competitions-schoolchild/> Режим доступа: свободный.
6. Академия Педагогики. Центр дистанционной поддержки учителей. – URL: <http://pedakademy.ru> Режим доступа: свободный.

7.4. Современные профессиональные базы данных и информационные справочные системы:

1. Электронно-библиотечная система издательства «Лань» – URL: <https://e.lanbook.com/> Режим доступа: по подписке ТюмГУ.

2. Электронно-библиотечная система Znaniyum.com – URL: <https://znaniyum.com/> Режим доступа: по подписке ТюмГУ.

3. IPR BOOKS – URL: <http://www.iprbookshop.ru/> Режим доступа: по подписке ТюмГУ.

4. Научная электронная библиотека eLIBRARY.RU – URL: <https://www.elibrary.ru/defaultx.asp> Режим доступа: по подписке ТюмГУ.

5. Межвузовская электронная библиотека (МЭБ) – URL: <https://icdlib.nspu.ru/> Режим доступа: по подписке ТюмГУ.

6. Национальная электронная библиотека (НЭБ) – URL: <https://rusneb.ru/> Режим доступа: по подписке ТюмГУ.

7. Ивис - – URL: <https://dlib.eastview.com/> Режим доступа: по подписке ТюмГУ.

8. Библиотека ТюмГУ - <https://library.utmn.ru/>

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

- Интернет-браузер для работы с интернет-ресурсами и информационными справочными системами;
- Microsoft Teams – интернет-приложение, платформа для электронного обучения.

Лицензионное ПО для разработки учебно-методических материалов:

– Microsoft Office 2003, Microsoft Office 2007, Microsoft Office 2010, Windows, Dr. Web, Autodesk AutoCAD 2018.

9. Технические средства и материально-техническое обеспечение дисциплины (модуля)

Мультимедийная учебная аудитория семинарского типа № 412 на 28 посадочных мест для проведения лекционных и практических занятий оснащена следующими техническими средствами обучения и оборудованием: учебная мебель, доска аудиторная, мультимедийное проекционное и акустическое оборудование, персональный компьютер **ПК** (DELL VOSTRO 3900: Intel Core i5-4460 3,2 ГГц; DDR3 4 ГБ; SSD 128 ГБ; DELL E2214НВ: 1920x1080; 21,5 дюйм; MS Windows 10; MS Office 2010), **проектор** (Epson EB-980W: 1280x800; 3800 лм), **экран** (16:9; 190x330 см)

На ПК установлено следующее программное обеспечение: Офисное ПО: операционная система MS Windows, офисный пакет MS Office, платформа MS Teams, офисный пакет LibreOffice, антивирусное ПО Dr. Web.

Обеспечено проводное подключение ПК к локальной сети и сети Интернет.

Мультимедийная учебная аудитория семинарского типа № 311 на 24 рабочих места с компьютерным классом на 15 рабочих мест для проведения индивидуальных и групповых консультаций, для самостоятельной работы оснащена следующими техническими средствами обучения и оборудованием:

15+1 ПК (Dell 3060-7601: Intel Core i5 8500T 2,1 ГГц; DDR4 8 ГБ; SSD 256 ГБ; Dell SE2216H: 1920x1080; 21,5 дюйма; MS Windows 10; MS Office 2010), **проектор** (Epson EB-980W: 1280x800; 3800 лм), **экран** (16:10)

На ПК установлено следующее программное обеспечение:

— Офисное ПО: операционная система MS Windows, офисный пакет MS Office, платформа MS Teams, офисный пакет LibreOffice, антивирусное ПО Dr. Web.

Обеспечено проводное подключение ПК к локальной сети и сети Интернет.