

Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Новгородский государственный университет имени Ярослава Мудрого»
Институт электронных и информационных систем

Кафедра алгебры и геометрии

УТВЕРЖДАЮ
Директор ИЭИС

 В.А. Шульцев

« 18 » 06 2024 г.

РАБОЧАЯ ПРОГРАММА
учебной дисциплины

АЛГЕБРА И ТЕОРИЯ ЧИСЕЛ

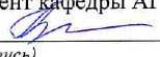
по направлению подготовки

01.03.01 Математика

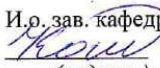
Направленность (профиль) **Математика в образовании, фундаментальных и прикладных исследованиях**

СОГЛАСОВАНО
Начальник отдела обеспечения
деятельности ИЭИС

 И.Н. Гуркова
(подпись)
« 05 » 06 2024 г.

Разработал
Доцент кафедры АГ
 Н.В. Неустроев
(подпись)
« 03 » 06 2024 г.

Принято на заседании кафедры АГ
Протокол № 11 от « 05 » 06 2024 г.

И.о. зав. кафедрой АГ
 Е.М. Кондрушенко
(подпись)
« 05 » 06 2024 г.

1 Цели и задачи освоения учебной дисциплины

Цели учебной дисциплины: формирование компетентности студентов в овладении математической и логической культурой теории чисел, числовых систем и теории вероятностей, позволяющей в дальнейшем успешно изучать основные математические дисциплины.

Задачи, решение которых обеспечивает достижение цели:

- формирование у студентов системы знаний по темам «Элементы теории делимости на множестве целых чисел», «Элементы теории сравнений», «Цепные дроби»;
- овладение основными понятиями тем «Элементы теории делимости на множестве целых чисел», «Элементы теории сравнений», «Цепные дроби»;
- формирование умений решать типовые задачи по темам «Элементы теории делимости на множестве целых чисел», «Элементы теории сравнений», «Цепные дроби»
- актуализация способности студентов использовать знания при решении реальных (смоделированных) математических задач;
- стимулирование студентов к самостоятельной деятельности по освоению дисциплины и формированию необходимых компетенций.

2 Место учебной дисциплины в структуре ОПОП

Учебная дисциплина алгебра и теория чисел (код блока Б1.О14) относится к обязательной части учебного плана основной профессиональной образовательной программы направления подготовки (специальности) 01.03.01 Математика и направленности (профилю) Математика в образовании, фундаментальных и прикладных исследованиях (далее – ОПОП). В качестве входных требований выступают сформированные ранее компетенции обучающихся, приобретенные ими в рамках следующих дисциплин (модулей, практик): Алгебра, Аналитическая геометрия. Освоение учебной дисциплины (модуля) является компетентностным ресурсом для дальнейшего изучения следующих дисциплин (модулей, практик): Теория чисел с приложениями в криптографии, Алгебра многочленов.

3 Требования к результатам освоения учебной дисциплины

Перечень компетенций, которые формируются в процессе освоения учебной дисциплины алгебра и теория чисел):

Общепрофессиональные компетенции:

ОПК-1 Способен применять фундаментальные знания, полученные в области математических и (или) естественных наук, и использовать их в профессиональной деятельности

Таблица 1 Результаты освоения учебной дисциплины:

Код и наименование компетенции	Результаты освоения учебной дисциплины (индикаторы достижения компетенций)		
	ОПК 1.1	ОПК 1.1	ОПК 1.3
ОПК-1 Способен применять фундаментальные знания, полученные в области математических и (или) естественных наук, и использовать их в профессиональной деятельности	Знает основные понятия и методы фундаментальных математических дисциплин	Умеет применять фундаментальные знания, полученные в области математических наук, и использовать их в профессиональной деятельности	Владеет умением осуществлять выбор методов решения задач профессиональной деятельности на основе теоретических знаний

4 Структура и содержание учебной дисциплины

4.1 Трудоемкость учебной дисциплины

Таблица 2 Трудоемкость учебной дисциплины алгебра и теория чисел для очной формы обучения:

Части учебной дисциплины (модуля)	Всего	Распределение по семестрам
		3 семестр
1. Трудоемкость учебной дисциплины (модуля) в зачетных единицах (ЗЕТ)	4	4
2. Контактная аудиторная работа в академических часах (АЧ)	42	42
3. Курсовая работа/курсовой проект (АЧ) (при наличии)	36	36
4. Внеаудиторная СРС в академических часах (АЧ)	30	30
5. Промежуточная аттестация (зачет; дифференцированный зачет; экзамен)	Экзамен 36	Экзамен 36

4.2 Содержание учебной дисциплины

Раздел № 1 Элементы теории делимости в кольце целых чисел

- 1.1. Деление нацело и с остатком
- 1.2. НОД и НОК целых чисел, алгоритм Евклида
- 1.3. Простые и составные числа. Основная теорема арифметики. Арифметические функции
- 1.4. Конечные цепные дроби. Диофантовы уравнения

Раздел № 2 Элементы теории групп

- 2.1. Подгруппы. Циклические подгруппы и группы.
- 2.2. Разложение группы по подгруппе. Теорема Лагранжа
- 2.3. Гомоморфизмы групп

Раздел № 3 Элементы теории сравнений

- 3.1. Отношение сравнимости в кольце целых чисел. Кольцо классов вычетов
- 3.2. Функция Эйлера, свойства. Теоремы Эйлера и Ферма
- 3.3. Сравнения первой степени. Способы решения сравнений. Системы сравнений
- 3.4. Сравнения высших степеней
- 3.5. Показатель числа, свойства. Первообразные корни, свойства
- 3.6. Индексы чисел, свойства, применение к решению сравнений
- 3.7. Квадратичные вычеты и невычеты. Символ Лежандра. Арифметические приложения теории сравнений

4.3 Трудоемкость разделов учебной дисциплины и контактной работы

Таблица 3 –Трудоемкость разделов учебной дисциплины
3 семестр

Наименование разделов (тем) учебной дисциплины (модуля), УЭМ, наличие КП/КР	Контактная работа (в АЧ)						Внеауд. СРС (в АЧ)	Форма текущего контроля
	Аудиторная			КР	в т.ч. СРС	ЭКЗ		
	ЛЕК	ПЗ	ЛР					
Раздел 1 Элементы теории делимости в кольце целых чисел								
1.1 Деление нацело и с остатком	1	2					2	ДР 1.1
1.2 НОД и НОК целых чисел, алгоритм Евклида	1	2	-		1		2	ДР 1.2
1.3 Простые и составные числа. Основная теорема арифметики. Арифметические функции	1	2	-		1		2	ДР 1.3
1.4 Конечные цепные дроби. Диофантовы уравнения	1	2	-				2	ДР 1.4 КЛ 1 КР 1
Раздел 2 Элементы теории групп								
2.1 Подгруппы. Циклические подгруппы и группы	1	2					2	ДР 2.1
2.2 Разложение группы по подгруппе. Теорема Лагранжа	1	2			1		2	ДР 2.2
2.3 Гомоморфизмы групп	1	2	-		1		2	ДР 2.3

Рубежная аттестация								Контрольный опрос - коллоквиум КЛ2 КР 2
ИТОГО	7	14			4		14	
Раздел 3 Элементы теории сравнений								
3.1 Отношение сравнимости в кольце целых чисел. Кольцо классов вычетов	1	2			1		2	ДР 3.1
3.2 Функция Эйлера, свойства. Теоремы Эйлера и Ферма	1	2			1		2	ДР 3.2
3.3 Сравнения первой степени. Способы решения сравнений. Системы сравнений	1	2					2	ДР 3.3
3.4 Сравнения высших степеней	1	2					2	ДР 3.4
3.5 Показатель числа, первообразные корни, индексы чисел свойства	1	2					2	ДР 3.5
3.6 Показатель числа, первообразные корни, свойства	1	2			1		3	ДР. 3.6
3.7 Индексы чисел, свойства, применение к решению сравнений								ДР 3.7
3.8 Квадратичные вычеты и невычеты. Символ Лежандра. Арифметические приложения теории сравнений	1	2			1		3	ДР 3.8
Курсовая работа				36				КР
Промежуточная аттестация: Экзамен						36		Экзамен
ИТОГО	7	14	0	36	4	36	16	
ВСЕГО	14	28	0	36	8	36	30	

4.4 Лабораторные работы и курсовые работы/курсовые проекты

4.4.1 Перечень тем лабораторных работ:

Лабораторные работы не предусмотрены учебным планом.

4.4.2 Примерные темы курсовых работ/курсовых проектов:

Курсовые работы/курсовые проекты не предусмотрены учебным планом.

Содержание курсовой работы

Этап 1. Обсуждение с руководителем предлагаемых тем. Работа с литературой. Постановка задачи.

Студент обсуждает с руководителем тему будущей курсовой работы, знакомится с постановкой задачей. В случае необходимости повторяет теоретический материал, изучает новый материал необходимый для успешного выполнения работы. В случае исследовательского характера работы знакомится с новейшими достижениями по теме работы в библиотеке и с использованием сети интернет.

Этап 2. Выполнение поставленных задач. Составление литературного обзора. Обсуждение полученных результатов.

Студент анализирует задачу, один или вместе с руководителем намечает пути решения. Составляет литературный обзор по теме курсовой. Периодически обсуждает полученные результаты с руководителем на консультациях или на научном семинаре. В случае возникновения недочетов исправляет их и снова обсуждает с руководителем.

Этап 3. Проверка полученных результатов на практике. Обсуждение полученных результатов.

Если курсовая работа носит прикладной характер и требует сопоставления полученных теоретических результатов с экспериментом или численными расчетами, то студент осуществляет это сопоставление. Результаты обсуждает с научным руководителем или на научном семинаре. В случае возникновения недочетов исправляет их и снова обсуждает с руководителем.

Этап 4. Оформление курсовой работы. Проверка на антиплагиат.

При выполнении основных задач, намеченных в курсовой работе, студент оформляет работу в соответствии с действующим ГОСТом. В курсовой работе должен быть титульный лист, введение, оглавление, основная часть, выводы и заключение, список используемой литературы, приложения (компьютерные программы и прочее).

5 Методические рекомендации по организации освоения учебной дисциплины

Таблица 4 – Темы лекционных занятий

№	Темы лекционных занятий (форма проведения)	Трудоемкость в АЧ
1	Деление нацело и с остатком (Структура деловой коммуникации (информационная лекция))	1
2	НОД и НОК целых чисел, алгоритм Евклида (Деловой стиль вербальной коммуникации (лекция-презентация))	1

3	Простые и составные числа. Основная теорема арифметики. Арифметические функции (Деловая этика и деловой этикет (проблемная лекция))	1
4	Конечные цепные дроби. Диофантовы уравнения (Структура деловой коммуникации (информационная лекция))	1
5	Подгруппы. Циклические подгруппы и группы. (Структура деловой коммуникации (информационная лекция))	1
6	Разложение группы по подгруппе. Теорема Лагранжа (Деловая этика и деловой этикет (проблемная лекция))	1
7	Гомоморфизмы групп(Структура деловой коммуникации (информационная лекция))	1
8	Отношение сравнимости в кольце целых чисел. Кольцо классов вычетов (Структура деловой коммуникации (информационная лекция))	1
9	Функция Эйлера, свойства. Теоремы Эйлера и Ферма (Структура деловой коммуникации (информационная лекция))	1
10	Сравнения первой степени. Способы решения сравнений. Системы сравнений (Структура деловой коммуникации (информационная лекция))	1
11	Сравнения высших степеней (Деловая этика и деловой этикет (проблемная лекция))	1
12	Показатель числа, первообразные корни, индексы чисел, свойства (Деловая этика и деловой этикет (проблемная лекция))	1
13	Индексы чисел, свойства, применение к решению сравнений (Структура деловой коммуникации (информационная лекция))	1
14	Квадратичные вычеты и невычеты. Символ Лежандра. Арифметические приложения теории сравнений (Деловая этика и деловой этикет (проблемная лекция))	1
ИТОГО		14

Таблица 5 – Темы практических занятий

№	Темы практических занятий (форма проведения)	Трудоемкость в АЧ
1	Деление нацело и с остатком (Невербальные виды деловой коммуникации (работа в группе))	2
2	НОД и НОК целых чисел, алгоритм Евклида(Невербальные виды деловой коммуникации (работа в группе))	2
3	Простые и составные числа. Основная теорема арифметики. Арифметические функции(Невербальные виды деловой коммуникации (работа в группе))	2
4	Конечные цепные дроби. Диофантовы уравнения(Невербальные виды деловой коммуникации (работа в группе))	2
5	Подгруппы. Циклические подгруппы и группы.(Невербальные виды деловой коммуникации (работа в группе))	2
6	Разложение группы по подгруппе. Теорема Лагранжа(Невербальные виды деловой коммуникации (работа в группе))	2
7	Гомоморфизмы групп (Невербальные виды деловой коммуникации (работа в группе))	2

7.	Сравнения первой степени. Способы решения сравнений. Системы сравнений(Невербальные виды деловой коммуникации (работа в группе))	2
8.	Сравнения высших степеней(Невербальные виды деловой коммуникации (работа в группе))	4
9.	Показатель числа, свойства. Первообразные корни, свойства(Невербальные виды деловой коммуникации (работа в группе))	2
10.	Индексы чисел, свойства, применение к решению сравнений (Невербальные виды деловой коммуникации (работа в группе))	4
11.	Квадратичные вычеты и невычеты. Символ Лежандра Арифметические приложения теории сравнений (Невербальные виды деловой коммуникации (работа в группе))	2
	ИТОГО	28

6 Фонд оценочных средств учебной дисциплины

Фонд оценочных средств представлен в Приложении А.

7 Условия освоения учебной дисциплины

7.1 Учебно-методическое обеспечение

Учебно-методического обеспечение учебной дисциплины представлено в Приложении Б.

7.2 Материально-техническое обеспечение

Таблица 6 – Материально-техническое обеспечение учебной дисциплины

№	Требование к материально-техническому обеспечению согласно ФГОС ВО	Наличие материально-технического оборудования	
1.	Учебные аудитории для проведения учебных занятий	аудитория для проведения лекционных и/или практических занятий: учебная мебель (столы, стулья, доска)	
		помещения для самостоятельной работы (наличие компьютера, выход в Интернет)	
2.	Мультимедийное оборудование	компьютер, проектор, экран, выход в интернет	
3.	Программное обеспечение		
Наименование программного продукта		Обоснование для использования (лицензия, договор, счёт, акт или иное)	Дата выдачи
ContentReader PDF 15 Business Версия для скачивания (годовая лицензия с академической скидкой) * <i>Только для осеннего семестра</i>		Договор №3КС/260	31.10.2023
Антиплагиат. Вуз.*		Договор №05//ЕП(У)24-ВБ	18.01.2024
MS Office 365		Безвозмездно передаваемое ВУЗам	-
Adobe Acrobat		свободно распространяемое	-
Teams		Входит в состав MS Office 365	-
Skype		свободно распространяемое	-
Zoom		свободно распространяемое	-
"Kaspersky Endpoint Security для бизнеса - Стандартный Russian Education Renewal. 250-499 Node I year License" /1 год *		Договор №294/ЕП(У)25-ВБ	13.09.2023
Astra Linux Special Edition*		195200041-alse-1.7-client-base_orel-x86_64-0-14211	09.12.2022
Astra Linux Special Edition*		195200041-alse-1.7-client-base_orel-x86_64-0-12617	21.11.2022
Astra Linux Special Edition*		195200041-alse-1.7-client-max-x86_64-0-11416	26.10.2022
Astra Linux Special Edition*		195200041-alse-1.7-client-base_orel-x86_64-0-9651	28.09.2022
Astra Linux Special Edition*		195200041-alse-1.7-client-base-x86_64-0-8801	07.09.2022
Astra Linux Special Edition*		195200041-alse-1.7-client-base-x86_64-0-8590	01.09.2022
* отечественное производство			

Приложение А
(обязательное)
Фонд оценочных средств
учебной дисциплины "Алгебра и теория чисел"

1 Структура фонда оценочных средств

Фонд оценочных средств состоит из двух частей:

а) открытая часть— общая информация об оценочных средствах (название оценочных средств, проверяемые компетенции, баллы, количество вариантов заданий, методические рекомендации для применения оценочных средств и пр.), которая представлена в данном документе, а также те вопросы и задания, которые могут быть доступны для обучающегося;

б) закрытая часть—фонд вопросов и заданий, которая не может быть заранее доступна для обучающихся (экзаменационные билеты, вопросы к контрольной работе и пр.) и которая хранится на кафедре.

2 Перечень оценочных средств текущего контроля и форм промежуточной аттестации

Таблица А.1 – Перечень оценочных средств

3 семестр

№	Оценочные средства для текущего контроля	Разделы (темы) учебной дисциплины	Баллы	Проверяемые компетенции
1	Контрольный опрос - коллоквиум - 1	1.1, 1.2	20	ОПК-1
	Контрольный опрос - коллоквиум - 2	1.3,1.4,1.5	20	
2	Контрольная работа - 1	1.1, 1.2	20	
	Контрольная работа - 2	1.3,1.4,1.5	20	
3	Домашняя работа	1.1,2.1	20	
4	Курсовая работа		50	
Промежуточная аттестация				
5	Экзамен	1.1, 1.2, 1.3, 1.4, 1.5	50	ОПК-1
	ИТОГО		200	

3 Рекомендации к использованию оценочных средств

Таблица А.2 – Контрольный опрос-коллоквиум (КЛ)

Критерии оценки		Количество вариантов заданий	Количество вопросов
10-12 баллов	испытывает трудности при демонстрации знаний, испытывает трудности в определениях терминов и описаниях алгоритмов действий	КЛ 1 - 12 КЛ 2 - 10	2
13-18 баллов	допускает неточности при изложении материала; не всегда четко дает определения терминов, имеет представление об алгоритмах действий		
19-20 баллов	имеет целостное представление об излагаемом материале, определения четкие, безошибочны алгоритмы действий		

Контрольные вопросы (КЛ 1)

- 1 Отношение делимости в $\mathbb{Z}$, свойства.
- 2 Деление с остатком. Теорема.
- 3 Системы счисления. Признаки делимости.
- 3 НОД целых чисел, свойства, алгоритм Евклида.
- 4 Свойства взаимно-простых чисел.
- 5 НОК целых чисел, свойства.
- 6 Простые и составные числа, свойства
- 7 Основная теорема арифметики. Распределение простых чисел.
- 8 Арифметические функции.
- 9 Конечные цепные дроби. Теорема.
- 10 Подходящие дроби, свойства.
- 11 Неопределенные (диофантовы) уравнения.

Контрольные вопросы к коллоквиуму (КЛ2)

1. Отношение сравнимости в Z , свойства.
2. Кольцо классов вычетов по заданному модулю.
3. Полная и приведенная системы вычетов, свойства.
4. Функция Эйлера и ее свойства. Теоремы Эйлера и Ферма.
5. Сравнения первой степени с одним неизвестным.
6. Способы решения сравнений первой степени.
7. Системы сравнений. Китайская теорема об остатках.
8. Сравнения n -ой степени (сведение решения сравнения по модулю степени простого к решению сравнения по простому модулю).
9. Теорема о числе решений сравнения n -ой степени. Следствие.

Таблица А.3–Контрольная работа (КР)

Критерии оценки		Количество вариантов заданий	Количество вопросов
Решил все задачи; Использовал математическую терминологию; Применил навыки обобщения и анализа; Свободно пользуется нужными формулами и приводит правильные определения.	«отлично»	4	10 (6) задания из соответствующего раздела
Использовал математическую терминологию; Не решил все задачи; Не полностью применил навыки анализа математической информации; Продemonстрировал некоторое знание о необходимом математическом аппарате.	«хорошо»		
Не решил все задачи; Не использовал навыки анализа математической информации; Не продемонстрировал знаний о необходимом математическом аппарате.	«удовлетворительно»		

Контрольная работа № 1

Вариант №1

- 1 Найдите, какие возможны остатки при делении числа $n_3 + 2$ ($n \in N$) на 9.
- 2 Докажите, что $S = 3^3 - 3^6 + 3^9 - \dots - 3^{6n}$, $n \in N$ делится на 13 при любом натуральном n .
- 3 Докажите, что остаток от деления простого числа на 30 – не составное число.
- 4 Найдите НОД и НОК для чисел (с помощью алгоритма Евклида и разложения на множители): 12606 и 6494.
- 5 Представьте в виде цепной дроби $\frac{875}{576}$.
- 6 Найдите значение цепной дроби $[0; 4, 1, 3, 2, 5]$.

- 7 Запишите числа a и b в системе счисления с основанием g и разделите большее на меньшее: $a = 132_4$, $b = 1643_7$, $g = 5$.
- 8 Разложите число 150 на два положительных слагаемых, одно из которых кратно 11, а второе – 17.
- 9 Исследуйте, какие числа при зачеркивании последней цифры уменьшаются в целое число раз.
- 10 Докажите, что при любом натуральном n выражение $(n^7 - n)$ делится на 42

Вариант № 2

- 1 Найдите остаток от деления натурального числа n на 45, если известно, что остатки от деления n на 15 и на 9 соответственно равны 2 и 5.
- 2 Докажите, что $S = 2^2 + 2^4 + 3^6 + \dots + 2^{8n}$, $n \in N$ делится на 17 при любом натуральном n .
- 3 Докажите, что если $(8n + 1)$ и $(24n + 1)$ - точные квадраты, то $(8n + 3)$ - составное число ($n > 1$, $n \in N$).
- 4 Найдите НОД и НОК для чисел (с помощью алгоритма Евклида и разложения на множители): 1403 и 1058.
- 5 Представьте в виде цепной дроби $-\frac{251}{764}$.
- 6 Найдите значение цепной дроби $[2; 1, 3, 4, 1, 2]$.
- 7 Запишите числа a и b в системе счисления с основанием g и разделите большее на меньшее: $a = 1653_7$, $b = 201_{10}$, $g = 4$.
- 8 Разложите число 134 на два положительных слагаемых, одно из которых кратно 13, а второе – 19.
- 9 Сколькими нулями оканчивается произведение чисел от 1 до n (включительно) при $n = 30, 58, 103$? Укажите общий прием решения задачи и воспользуйтесь им для случая $n = 1976$.
- 10 Докажите, что при любом натуральном n выражение $(9^n - 8n - 1)$ делится на 64.

Контрольная работа № 2.

Вариант 1

- 1 Найти остаток от деления :
 34^{3741} на 26

- 2 Решить сравнения:

- а) $15x \equiv 21 \pmod{18}$
б) $95x \equiv 59 \pmod{308}$

- 3 Найти первообразные корни по модулю (если они существуют):

$$m = 11$$

- 4 вычислить символ Лежандра:

$$\left(\frac{241}{593} \right)$$

- 5 Найти длину периода и предпериода при обращении обыкновенной дроби в десятичную:

$$\frac{17}{24}$$

Вариант 2

$$178^{2741} \text{ на } 22$$

- а) $20x \equiv 35 \pmod{45}$
б) $91x \equiv 1 \pmod{132}$

$$m = 13$$

$$\frac{251}{577}$$

$$\frac{12}{35}$$

6 Решить сравнение с помощью индексов:

$$7x^4 \equiv 10 \pmod{17}$$

$$40x^{10} \equiv 3 \pmod{17}$$

Таблица А.4 – Домашняя работа (ДР)

Критерии оценки		Количество заданий
Знание и понимание теоретического содержания курса с незначительными пробелами; несформированность некоторых практических умений при применении знаний в конкретных ситуациях, низкое качество выполнения учебных заданий (не выполнены, либо оценены числом баллов, близким к минимальному).	«удовлетворительно»	2 из контролируемого раздела
Полное знание и понимание теоретического содержания курса, без пробелов; недостаточную сформированность некоторых практических умений при применении знаний в конкретных ситуациях; достаточное качество выполнения всех предусмотренных программой обучения учебных заданий (ни одного из них не оценено минимальным числом баллов, некоторые виды заданий выполнены с ошибками);	«хорошо»	
Полное знание и понимание теоретического содержания курса, без пробелов; сформированность необходимых практических умений при применении знаний в конкретных ситуациях, высокое качество выполнения всех предусмотренных программой обучения учебных заданий (оценены числом баллов, близким к максимальному);	«отлично»	

Темы домашней работы 1.1:

1. Основные свойства отношения делимости целых чисел.
2. Основные свойства простых чисел. Решето Эратосфена.
3. Основные свойства НОД и НОК целых чисел и взаимно простых чисел.
4. Арифметические функции.
5. Неопределенные (диофантовы) уравнения.

Задачи для домашней работы

- 1 Найдите, какие возможны остатки при делении числа $n_3 + 2$ ($n \in N$) на 9.
- 2 Докажите, что $S = 3^3 - 3^6 + 3^9 - \dots - 3^{6n}$, $n \in N$ делится на 13 при любом натуральном n .
- 3 Найдите НОД и НОК для чисел (с помощью алгоритма Евклида и разложения на множители): 12606 и 6494.
- 4 Представьте в виде цепной дроби $\frac{875}{576}$. Найдите значение цепной дроби $[0; 4, 1, 3, 2, 5]$.

Темы домашней работы 1.2:

1. Полная и приведенная система вычетов.
2. Способы решения сравнений первой степени.
3. Квадратичные вычеты и невычеты.
4. Свойства символа Лежандра и Якоби.
5. Бесконечные цепные дроби. Квадратические иррациональности.

Задачи для домашней работы

- 1 Найти остатки от деления:
 - 1) 293^{275} на 48.1; 2) 109^{345} на 14
- 2 Решите следующие сравнения:

1) $12 \cdot x \equiv 1 \pmod{7}$; 2) $6 \cdot x \equiv 3 \pmod{7}$; 3) $10 \cdot x \equiv 25 \pmod{35}$;

3 Решить двучленные уравнения с помощью индексов:

1) $3 \cdot x^3 \equiv 4 \pmod{7}$; 2) $25 \cdot x^7 \equiv -7 \pmod{31}$; 3) $40 \cdot x^{10} \equiv 3 \pmod{17}$;

4 Решить с помощью индексов степенные сравнения.

1) $32^x \equiv 15 \pmod{37}$; 2) $25^{5 \cdot x} \equiv 47 \pmod{31}$.

5 Вычислить символ Лежандра:

1) $\left(\frac{63}{131}\right)$; 2) $\left(\frac{35}{97}\right)$; 3) $\left(\frac{29}{383}\right)$; 4) $\left(\frac{241}{593}\right)$; 5) $\left(\frac{257}{571}\right)$;

6) $\left(\frac{251}{577}\right)$; 7) $\left(\frac{342}{677}\right)$.

6) Вычислением символа Лежандра установить, какие из следующих сравнений разрешимы и найти их решения:

1) $x^2 \equiv 6 \pmod{7}$; 2) $x^2 \equiv 12 \pmod{13}$; 3) $x^2 \equiv 13 \pmod{17}$.

Таблица А.5 – Экзамен

Критерии оценки		Количество вариантов	Количество вопросов
знание и понимание теоретического содержания курса с незначительными пробелами; несформированность некоторых практических умений при применении знаний в конкретных ситуациях, низкое качество выполнения учебных заданий (не выполнены, либо оценены числом баллов, близким к минимальному); низкий уровень мотивации учения;	«удовлетворительно»	14	3
полное знание и понимание теоретического содержания курса, без пробелов; недостаточную сформированность некоторых практических умений при применении знаний в конкретных ситуациях; достаточное качество выполнения всех предусмотренных программой обучения учебных заданий (ни одного из них не оценено минимальным числом баллов, некоторые виды заданий выполнены с ошибками); средний уровень мотивации учения;	«хорошо»		
полное знание и понимание теоретического содержания курса, без пробелов; сформированность необходимых практических умений при применении знаний в конкретных ситуациях, высокое качество выполнения всех предусмотренных программой обучения учебных заданий (оценены числом баллов, близким к максимальному); высокий уровень мотивации учения.	«отлично»		

Б.1 Вопросы к экзамену по дисциплине «Алгебра и теория чисел» (3 семестр)

1 Отношение делимости в $\mathbb{Z}$, свойства.

2 Деление с остатком. Теорема.

3 Системы счисления. Признаки делимости.

11 НОД целых чисел, свойства, алгоритм Евклида.

12 Свойства взаимно-простых чисел.

- 13 НОК целых чисел, свойства.
- 14 Простые и составные числа, свойства
- 15 Основная теорема арифметики. Распределение простых чисел.
- 16 Арифметические функции.
- 17 Конечные цепные дроби. Теорема.
- 18 Подходящие дроби, свойства.
- 19 Неопределенные (диофантовы) уравнения.
- 20 Отношение сравнимости в $\mathbb{Z}$, свойства.
- 21 Кольцо классов вычетов по заданному модулю.
- 22 Полная и приведенная системы вычетов, свойства.
- 23 Функция Эйлера и ее свойства.
- 24 Теоремы Эйлера и Ферма.
- 25 Сравнения первой степени с одним неизвестным.
- 26 Способы решения сравнений первой степени.
- 27 Системы сравнений. Китайская теорема об остатках.
- 20 Сравнения n -ой степени (сведение решения сравнения по модулю степени простого к решению сравнения по простому модулю).
- 21 Теорема о числе решений сравнения n -ой степени. Следствие.
- 22 Сравнения второй степени. Квадратичные вычеты и невычеты. Число решений сравнения.
- 23 Критерий Эйлера для квадратичных вычетов и невычетов. 24 Символ Лежандра, его свойства.
- 24 Квадратичный закон взаимности.
- 25 Теорема Вильсона, теорема Лейбница (и другие критерии простоты числа).
- 26 Показатель числа по заданному модулю, его свойства.
- 27 Существование первообразного корня по простому модулю.
- 28 Теоремы о количестве чисел, принадлежащих показателю, и первообразных корней по заданному модулю.
- 29 Индексы (дискретный логарифм) по заданному модулю, их свойства.
- 30 Решение двучленных (степенных) сравнений и показательных сравнений с помощью индексов.
- 31 Арифметические приложения: а) нахождение остатков от деления некоторого числа на заданное число, б) признаки делимости, в) систематические дроби (определение длины периода при обращении обыкновенной дроби в десятичную дробь), г) проверка результатов арифметических действий, д) приложения теории чисел в криптографии.
- 32 Бесконечные цепные дроби. Подходящие дроби бесконечно цепных дробей, их свойства.
- 33 Разложение действительного числа в бесконечную цепную дробь.
- 34 Квадратические иррациональности. Периодические цепные дроби.
- 35 Теорема Лагранжа о разложении квадратичных иррациональностей в цепные дроби.
- 36 Разложение числа $\frac{e+1}{e-1}$ в бесконечную цепную дробь.
- 37 Разложение числа e в бесконечно цепную дробь.
- 38 Чисто периодические цепные дроби.
- 39 Приближение действительных чисел рациональными дробями. Теорема Дирихле. Теорема Гурвица.

Все материалы для проведения промежуточного контроля хранятся на кафедре.

Пример экзаменационного билета:

Новгородский государственный университет имени Ярослава Мудрого
 Институт электронных и информационных систем
 Кафедра алгебры и геометрии

Экзаменационный билет № 1

Учебная дисциплина «**Алгебра и теория чисел**»

Для направления подготовки (специальности) 01.03.01 Математика

Направленность (профиль) Математика в образовании, фундаментальных и прикладных исследованиях

1 НОД и НОК целых чисел, алгоритм Евклида

2 Теоремы Эйлера и Ферма

3 Решить сравнение

Принято на заседании кафедры «____» _____ 20__ г.

Протокол № _____

Заведующий кафедрой _____ (ФИО)

Таблица А.6 – Курсовая работа

Критерии оценки	
25–34 балла	недостаточно полно раскрыты основные вопросы избранной темы, допущены серьёзные неточности при изложении содержания работы и ответе на вопросы
35–44 балла	продемонстрировано полное владение материалом исследования, допущены некоторые несущественные неточности при изложении содержания работы, ответы на вопросы неполные
45–50 баллов	продемонстрировано полное владение материалом исследования, при изложении содержания работы и ответе на вопросы ошибок не допущено

Примерные темы курсовых работ/курсовых проектов:

1. Тестирование чисел на простоту

Приложение Б
(обязательное)
**Карта учебно-методического обеспечения
учебной дисциплины "Алгебра и теория чисел"**

Таблица 1 – Основная литература

<i>Библиографическое описание издания (автор, наименование, вид, место и год издания, кол. стр.)</i>	<i>Кол. экз. в библ. НовГУ</i>	<i>Наличие в ЭБС</i>
Печатные источники		
1 Бухштаб А.А. Теория чисел Учебное пособие. – СПб.: Лань, 2008. – 384 с.	3	
2 Виноградов И.М. Основы теории чисел. СПб.: Лань, 2004. – 176 с.	5	
3 Шнеперман Л.Б. Сборник задач по алгебре и теории чисел: Учебное пособие. – СПб.: Лань, 2008. – 222 с.	31	
4 Теория чисел: Книга для студентов специальности «учитель математики», «прикладная математика», «ПОВТ» / Н.В. Неустроев; О.Н. Неустроева; Новгородский государственный университет имени Ярослава Мудрого. – Великий Новгород, 2004. – 161 с.	5	
Электронные ресурсы		
1 Теория чисел : книга для студентов специальности Педагогическое образование. Математика и информатика./автор-составитель Н. В. Неустроев ; Новгородский государственный университет им. Ярослава Мудрого. – Великий Новгород, 2018. – 201 с. – Текст : электронный // ЭБС НовГУ. – URL : https://novsu.bookonline.ru/viewer/51954 . – Режим доступа : для авторизованных пользователей		ЭБС НовГУ

Таблица 2 – Дополнительная литература

<i>Библиографическое описание издания (автор, наименование, вид, место и год издания, кол. стр.)</i>	<i>Кол. экз. в библ. НовГУ</i>	<i>Наличие в ЭБС</i>
Печатные источники		
1 Неустроев Н.В. Элементы прикладной теории чисел: книга для студентов специальности «учитель математики» и «прикладная математика» / Автор Н.В. Неустроев; Новгородский государственный университет имени Ярослава Мудрого. – Великий Новгород, 2007. – 188 с.	4	

Таблица Б.3 – Информационное обеспечение модуля

<i>Наименование ресурса</i>	<i>Договор</i>	<i>Срок договора</i>
Электронная библиотека НовГУ		
Электронный каталог научной библиотеки http://mars.novsu.ac.ru/MarcWeb/	База собственной генерации	бессрочный
База данных «Аналитика» (картотека статей) http://mars.novsu.ac.ru/MarcWeb/	База собственной генерации	бессрочный
ЭБС «Электронная библиотечная система Новгородского государственного университета» (ЭБС НовГУ). Универсальный ресурс. Внутривузовские издания НовГУ.	Договор № 230 от 30.12.2022 с ООО «КДУ»	бессрочный

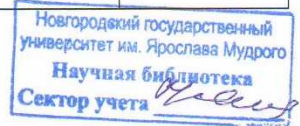
Новгородский государственный
университет им. Ярослава Мудрого
Научная библиотека
Сектор учета

Наименование ресурса	Договор	Срок договора
ЭБС «Лань» Единая профессиональная база данных для классических вузов – Издательство Лань «ЭБС» ЭБС ЛАНЬ	Договор № 34/ЕП(Т)23 от 22.12.2023 с ООО «Издательство ЛАНЬ»	с 01.01.2024 по 31.12.2024
ЭБС «ЛАНЬ» Коллекции: «Физика – Издательство МГТУ им. Н.Э.Баумана», «Информатика - Издательство ДМК Пресс», «Журналистика и медиа-бизнес - Издательство Аспект Пресс»	Договор № 33/ЕП(У)23 от 25.12.2023 с ООО «ЭБС ЛАНЬ»	с 01.01.2024 по 31.12.2024
ЭБС «ЛАНЬ» Универсальный ресурс	Договор № СЭБ НВ-283 с ООО «ЭБС ЛАНЬ» от 09.11.2020	с 09.11.2020 по 31.12.2023 Договор продлен до 31.12.2024 (основание: п.6.1.)
«ЭБС ЮРАЙТ www.biblio-online.ru» Универсальный ресурс.	Договор № 35/ЕП(У)23 от 25.12.2023 с ООО «Электронное издательство ЮРАЙТ»	с 01.01.2024 по 31.12.2024
«Национальная электронная библиотека» Универсальный ресурс.	Договор №101/НЭБ/2338П от 14.03.2022 с ФБГУ «Российская Государственная библиотека»	с 14.03.2022 по 13.03.2027
ЭБС «IPRsmart» Универсальный ресурс.	Лицензионный договор № 11040/23П/31/ЕП(У)23 от 22.12.2023 с ООО Компания «Ай Пи Ар Медиа»	с 01.01.2024 по 31.12.2024
ЭБС «IPRsmart» Электронно-образовательный ресурс для иностранных студентов «РУССКИЙ ЯЗЫК КАК ИНОСТРАННЫЙ» (РКИ).	Договор № 436/ЕП(У)23-ВБ от 15.12.2023 с ООО Компания «Ай Пи Ар Медиа»	с 01.01.2024 по 31.01.2025
ЭБС Polpred.com. Обзор СМИ. Электронные статьи 600 деловых газет, журналов, информагентств за 20 лет.	Соглашение с ООО «ПОЛПРЕД Справочники». Тестовый доступ.	с 01.01.2023
Профессиональные базы данных		
Президентская библиотека им. Б. Н. Ельцина https://www.prlib.ru/	в открытом доступе	-
База данных Научной электронной библиотеки eLIBRARY.RU https://elibrary.ru/	в открытом доступе	-
База данных профессиональных стандартов Министерства труда и социальной защиты РФ http://profstandart.rosmintrud.ru/obshchiy-informatsionnyy-blok/natsionalnyy-reestr-professionalnykh-standartov/	в открытом доступе	-
База данных электронно-библиотечной системы «Национальная электронная библиотека» https://нэб.рф	в открытом доступе	-
Информационные справочные системы		
Университетская информационная система «РОССИЯ» https://lib.tusur.ru/ru/resursy/bazy-dannyh/uis-rossiya	в открытом доступе	-
Национальный портал онлайн обучения «Открытое образование» https://openedu.ru	в открытом доступе	-

Новгородский государственный
университет им. Ярослава Мудрого
Научная библиотека
Сектор учета

Наименование ресурса	Договор	Срок договора
Портал открытых данных Российской Федерации https://data.gov.ru	в открытом доступе	-
Справочно-правовая система КонсультантПлюс (КонсультантПлюс студенту и преподавателю) www.consultant.ru/edu/	в открытом доступе	-

Проверено НБ НовГУ



И.о. зав. кафедрой АГ Е.М.Кондрушенко

подпись

И.О.Фамилия

« 05 » 06 20 24 г.

Рабочая программа актуализирована на 20__/20__ учебный год.
Протокол № ____ заседания кафедры от «____» _____ 20__ г.
Разработчик: _____
Зав. кафедрой _____

Рабочая программа актуализирована на 20__ / 20__ учебный год.
Протокол № ____ заседания кафедры от « ____ » _____ 20__ г.
Разработчик: _____
Зав. кафедрой _____

Рабочая программа актуализирована на 20__/20__ учебный год.
 Протокол № ____ заседания кафедры от «____» _____ 20__ г.
 Разработчик: _____
 Зав. кафедрой _____

[illegible]