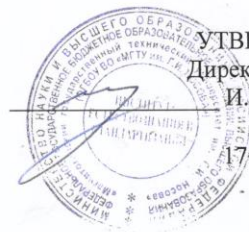




МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Магнитогорский государственный технический университет им. Г.И. Носова»



УТВЕРЖДАЮ
Директор ИЕиС
И.Ю. Мезин

17.02.2020 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

ТЕОРИЯ ЧИСЕЛ

Направление подготовки (специальность)
44.03.05 Педагогическое образование (с двумя профилями подготовки)

Направленность (профиль/специализация) программы
Математика и информатика

Уровень высшего образования - бакалавриат

Форма обучения
очная

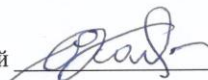
Институт/ факультет	Институт естествознания и стандартизации
Кафедра	Прикладной математики и информатики
Курс	3
Семестр	5

Магнитогорск
2020 год

Рабочая программа составлена на основе ФГОС ВО - бакалавриат по направлению подготовки 44.03.05 Педагогическое образование (с двумя профилями подготовки) (приказ Минобрнауки России от 22.02.2018 г. № 125)

Рабочая программа рассмотрена и одобрена на заседании кафедры Прикладной математики и информатики

11.02.2020, протокол № 6

Зав. кафедрой  С.И. Кадченко

Рабочая программа одобрена методической комиссией ИЕиС

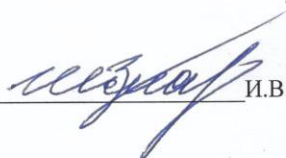
17.02.2020 г. протокол № 6

Председатель  И.Ю. Мезин

Рабочая программа составлена:

доцент кафедры ПМИИ, канд. физ.-мат. наук  Л.В.Смирнова

Рецензент:

директор МОУ СОШ № 33, канд. пед. наук  И.В.Шманева

Лист актуализации рабочей программы

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2021 - 2022 учебном году на заседании кафедры Прикладной математики и информатики

Протокол от _____ 20__ г. № ____
Зав. кафедрой _____ С.И. Кадченко

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2022 - 2023 учебном году на заседании кафедры Прикладной математики и информатики

Протокол от _____ 20__ г. № ____
Зав. кафедрой _____ С.И. Кадченко

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2023 - 2024 учебном году на заседании кафедры Прикладной математики и информатики

Протокол от _____ 20__ г. № ____
Зав. кафедрой _____ С.И. Кадченко

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2024 - 2025 учебном году на заседании кафедры Прикладной математики и информатики

Протокол от _____ 20__ г. № ____
Зав. кафедрой _____ С.И. Кадченко

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2025 - 2026 учебном году на заседании кафедры Прикладной математики и информатики

Протокол от _____ 20__ г. № ____
Зав. кафедрой _____ С.И. Кадченко

1 Цели освоения дисциплины (модуля)

формирование способности осуществлять педагогическую деятельность на основе специальных научных знаний. Содержание дисциплины направлено на освоение фундаментальных понятий и результатов теории делимости в кольце целых чисел, теории сравнений, теории цепных дробей, квадратичных вычетов, первообразных корней и индексов, о распределении простых чисел, формирование умений и навыков в решении задач из этих разделов теории чисел; развитие навыков в постановке и решении практических задач, знакомство с основными вычислительными алгоритмами теории чисел.

2 Место дисциплины (модуля) в структуре образовательной программы

Дисциплина Теория чисел входит в обязательную часть учебного плана образовательной программы.

Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:

Дискретная математика

Алгебра

Математический анализ

Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:

Дискретная математика

Методика обучения математики в школе

Элементарная математика

Подготовка к сдаче и сдача государственного экзамена

3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения

В результате освоения дисциплины (модуля) «Теория чисел» обучающийся должен обладать следующими компетенциями:

Код индикатора	Индикатор достижения компетенции
ОПК-8	Способен осуществлять педагогическую деятельность на основе специальных научных знаний
ОПК-8.1	Планирует и проводит научные исследования в области педагогической деятельности
ОПК-8.2	Использует специальные научные знания для повышения эффективности педагогической деятельности

4. Структура, объём и содержание дисциплины (модуля)

Общая трудоемкость дисциплины составляет 2 зачетных единиц 72 акад. часов, в том числе:

- контактная работа – 39,05 акад. часов;
- аудиторная – 38 акад. часов;
- внеаудиторная – 1,05 акад. часов
- самостоятельная работа – 32,95 акад. часов;

Форма аттестации - зачет

Раздел/ тема дисциплины	Семестр	Аудиторная контактная работа (в акад. часах)			Самостоятельная работа студента	Вид самостоятельной работы	Форма текущего контроля успеваемости и промежуточной аттестации	Код компетенции
		Лек.	лаб. зан.	практ. зан.				
1. Делимость в кольце целых чисел.								
1.1 Свойства делимости в кольцах. Группа обратимых элементов кольца. Деление с остатком целых чисел. Наибольший общий делитель. Наименьшее общее кратное. Алгоритм Евклида. Наименьшее общее кратное. Алгоритм Евклида.	5	6		6/4И	4	Подготовка к практическому занятию. Выполнение практических работ (решение задач, письменных работ)	Устный опрос, проверка индивидуальных заданий, самостоятельная работа. контрольная работа	ОПК-8.2, ОПК-8.1
1.2 Простые числа. Решето Эратосфена. Факториальность кольца целых чисел. Целая и дробная части числа. Порядок простого множителя в $n!$.		2		2/2И	4	Подготовка к практическому занятию. Выполнение практических работ (решение задач, письменных работ)	Устный опрос, проверка индивидуальных заданий, самостоятельная работа. контрольная работа	ОПК-8.2, ОПК-8.1
Итого по разделу		8		8/6И	8			
2. Теория сравнений.								
2.1 Классы вычетов по $\text{mod } m$. Кольцо классов вычетов. Поле классов вычетов по простому модулю. Обратимые элементы кольца классов вычетов. Функция Эйлера. Теорема Эйлера. Малая теорема Ферма. Теорема Вильсона. Решение сравнений 1-й	5	4		4/2И	8	Подготовка к практическому занятию. Выполнение практических работ (решение задач, письменных работ)	Устный опрос, проверка индивидуальных заданий, самостоятельная работа. контрольная работа	ОПК-8.2, ОПК-8.1

2.2 Мультипликативность функции Эйлера. Китайская теорема об остатках. Основные мультипликативные теоретико-числовые функции: функция Мебиуса, сумма делителей натурального числа, количество делителей. Формула обращения Мебиуса		2		2	8	Подготовка к практическому занятию. Выполнение практических работ (решение задач, письменных работ)	Устный опрос, проверка индивидуальных заданий, самостоятельная работа. контрольная работа	ОПК-8.2, ОПК-8.1
Итого по разделу	6		6/2И	16				
3. Цепные дроби.								
3.1 Алгоритм Евклида и разложение рационального числа в цепную дробь. Разложение в цепную дробь вещественного числа. Свойства подходящих дробей. Квадратичные иррациональности и периодические цепные дроби	5	2		4/2И	4	Подготовка к практическому занятию. Выполнение практических работ (решение задач, письменных работ)	Устный опрос, проверка индивидуальных заданий, самостоятельная работа. контрольная работа	ОПК-8.2, ОПК-8.1
3.2 Решение уравнений 1-й степени в целых числах. Применение цепных дробей к решению сравнений 1-й степени. Наилучшие приближения рациональными числами.		3		1	4,95	Подготовка к практическому занятию. Выполнение практических работ (решение задач, письменных работ)	Устный опрос, проверка индивидуальных заданий, самостоятельная работа. контрольная работа	ОПК-8.2, ОПК-8.1
Итого по разделу	5		5/2И	8,95				
Итого за семестр	19		19/10И	32,95			зачёт	
Итого по дисциплине	19		19/10И	32,95			зачет	

5 Образовательные технологии

При проведении занятий и организации самостоятельной работы студентов используются:

1. Традиционные образовательные технологии, ориентированные на организацию образовательного процесса и предполагающую прямую трансляцию знаний от преподавателя к студенту.

Формы учебных занятий с использованием традиционных технологий:

Информационная лекция – последовательное изложение материала в дисциплинарной логике, осуществляемое преимущественно вербальными средствами (монолог преподавателя).

Практическое занятие, посвященное освоению конкретных умений и навыков по предложенному алгоритму.

2. Технологии проблемного обучения – организация образовательного процесса, которая предполагает постановку проблемных вопросов, создание учебных проблемных ситуаций для стимулирования активной познавательной деятельности студентов.

Формы учебных занятий с использованием технологий проблемного обучения:

Практическое занятие в форме практикума – организация учебной работы, направленная на решение комплексной учебно-познавательной задачи, требующей от студента применения как научно-теоретических знаний, так и практических навыков.

3. Интерактивные технологии – организация образовательного процесса, которая предполагает активное и нелинейное взаимодействие всех участников, достижение на этой основе лично значимого для них образовательного результата.

Формы учебных занятий с использованием специализированных интерактивных технологий: Лекция «обратной связи» – лекция–провокация (изложение материала с заранее запланированными ошибками), лекция-беседа.

4. Информационно-коммуникационные образовательные технологии – организация образовательного процесса, основанная на применении программных сред и технических средств работы с информацией по теме научно-исследовательской работы студента.

Формы учебных занятий с использованием информационно-коммуникационных технологий:

Лекция-визуализация – изложение содержания сопровождается презентацией и видеоматериалов

6 Учебно-методическое обеспечение самостоятельной работы обучающихся

Представлено в приложении 1.

7 Оценочные средства для проведения промежуточной аттестации

Представлены в приложении 2.

8 Учебно-методическое и информационное обеспечение дисциплины (модуля)

а) Основная литература:

1. Виноградов, И. М. Основы теории чисел / И. М. Виноградов. — Москва : Издательство Юрайт, 2020. — 123 с. — (Антология мысли). — ISBN 978-5-534-12085-1. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: <https://urait.ru/bcode/447009> (дата обращения: 30.09.2020).

2. Сикорская Г.А. Алгебра и теория чисел / Г.А. Сикорская. - Оренбург : Оренбургский государственный университет, 2017. - 303 с. - ISBN 978-5-7410-1943-6. - URL: <https://ibooks.ru/bookshelf/364740/reading> (дата обращения: 30.09.2020). - Текст: электронный.

3. Смолин Ю.Н. Алгебра и теория чисел : учеб. пособие / Ю.Н. Смолин. - Москва : Флинта, 2012. - 464 с. - ISBN 978-5-9765-0050-1. - URL: <https://ibooks.ru/bookshelf/27168/reading> (дата обращения: 30.09.2020). - Текст: электронный.

б) Дополнительная литература:

1. Лось, А. Б. Криптографические методы защиты информации для изучающих компьютерную безопасность : учебник для вузов / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. — 2-е изд., испр. — Москва : Издательство Юрайт, 2020. — 473 с. — (Высшее образование). — ISBN 978-5-534-12474-3. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: <https://urait.ru/bcode/450277> (дата обращения: 30.09.2020).

2. Ларин, С. В. Алгебра и теория чисел. Группы, кольца и поля : учебное пособие для вузов / С. В. Ларин. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2020. — 160 с. — (Высшее образование). — ISBN 978-5-534-05567-2. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: <https://urait.ru/bcode/454465> (дата обращения: 30.09.2020).

3. Чебышёв, П. Л. Теория чисел. Теория вероятностей. Теория механизмов / П. Л. Чебышёв ; ответственный редактор И. М. Виноградов ; составитель А. О. Гельфонд. — Москва : Издательство Юрайт, 2020. — 457 с. — (Антология мысли). — ISBN 978-5-534-05214-5. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: <https://urait.ru/bcode/454232> (дата обращения: 30.09.2020).

в) Методические указания:

1. Пантина И.В. Алгебра и теория чисел / И.В. Пантина, М.А. Куприянова, С.В. Харитонов. - Москва : МФПУ «Синергия», 2016. - 160 с. - ISBN 978-5-4257-0253-1. - URL: <https://ibooks.ru/bookshelf/353808/reading> (дата обращения: 30.09.2020). - Текст: электронный.

2. Балюкевич Э. Л. Алгебра и теория чисел: учебное пособие / Э.Л. Балюкевич. - Москва : ЕАОИ, 2011. - 278 с. - ISBN 978-5-374-00535-6. - URL: <https://ibooks.ru/bookshelf/334400/reading> (дата обращения: 30.09.2020). - Текст: электронный.

г) Программное обеспечение и Интернет-ресурсы:

Программное обеспечение

Наименование ПО	№ договора	Срок действия лицензии
MS Office 2007 Professional	№ 135 от 17.09.2007	бессрочно
7Zip	свободно распространяемое	бессрочно

Профессиональные базы данных и информационные справочные системы

Название курса	Ссылка
Электронная база периодических изданий East View Information Services, ООО «ИВИС»	https://dlib.eastview.com/
Национальная информационно-аналитическая система – Российский индекс научного цитирования (РИНЦ)	URL: https://elibrary.ru/project_risc.asp
Поисковая система Академия Google (Google Scholar)	URL: https://scholar.google.ru/
Российская Государственная библиотека. КATALOGI	https://www.rsl.ru/ru/4readers/catalogues/

Электронные ресурсы библиотеки МГТУ им. Г.И. Носова	http://magtu.ru:8085/marcweb2/Default.asp
Международная реферативная и полнотекстовая справочная база данных научных из-	http://scopus.com
Международная наукометрическая реферативная и полнотекстовая база данных научных изданий «Web of science»	http://webofscience.com

9 Материально-техническое обеспечение дисциплины (модуля)

Материально-техническое обеспечение дисциплины включает:

Учебные аудитории для проведения занятий лекционного типа.

Доска, мультимедийный проектор, экран.

Учебные аудитории для проведения лабораторных занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Персональные компьютеры с пакетом MS Office, вы-ходом в Интернет и с доступом в электронную информационно-образовательную среду университета.

Комплекс тестовых заданий для проведения рубежного и промежуточного контроля.

Помещения для самостоятельной работы обучающихся.

Персональные компьютеры с пакетом MS Office, выходом в Интернет и с доступом в электронную информационно-образовательную среду университета.

Помещения для хранения и профилактического обслуживания учебного оборудования.

Шкафы для хранения учебно-методической документации, учебного оборудования и учебно-наглядных пособий.

Приложение 1

6. Учебно-методическое обеспечение самостоятельной работы обучающихся

Раздел/ тема дисциплины	Вид самостоятельной работы	Кол-во часов	Формы контроля
1. Делимость в кольце целых чисел.			
1.1. Свойства делимости в кольцах. Группа обратимых элементов кольца. Деление с остатком целых чисел. Наибольший общий делитель. Наименьшее общее кратное. Алгоритм Евклида..	Самостоятельное изучение учебной литературы. Изучение темы: Неравенства Чебышева. Асимптотический закон распределения простых чисел.	4	Текущий контроль Конспект
1.2. Простые числа. Решето Эратосфена. Факториальность кольца целых чисел. Целая и дробная части числа. Порядок простого множителя в $n!$.	Разработать конспект урока на тему Простые и составные числа. Написать программу получения простых чисел в заданном диапазоне.	4	Проверка конспекта. Проверка программы
Итого по разделу		8	
2. Теория сравнений.			
2.1. Классы вычетов по mod m . Кольцо классов вычетов. Поле классов вычетов по простому модулю. Обратимы елемен-	Разработка конспекта серии уроков на тему Сравнения. Решение сравнений первой степени. Изучить самостоятельно тему Квадратичные вычеты	8	Текущий контроль Конспект

ты кольца классов вычетов. Функция Эйлера. Теорема Эйлера. Малая теорема Ферма. Теорема Вильсона. Решение сравнений 1-й степени.	и невычеты по mod p . Символ Лежандра. Квадратичный закон взаимности Гаусса		
2.2. Мультипликативность функции Эйлера. Китайская теорема об остатках. Основные мультипликативные теоретико-числовые функции: функция Мебиуса, сумма делителей натурального числа, количество делителей. Формула обращения Мебиуса.	Разработка программы, вычисляющей значения мультипликативных функций.	8	Текущий контроль Конспект
Итого по разделу		8	
3. Цепные дроби.			
3.1. Алгоритм Евклида и разложение рационального числа в цепную дробь. Разложение в цепную дробь вещественного числа. Свойства подходящих дробей. Квадратичные иррациональности и периодические цепные дроби.	Составить программу, осуществляющую разложение рационального числа в цепную дробь.	6	Проверка конспекта. Проверка программы
3.2. Решение уравнений 1-й степени в целых числах. Применение цепных дробей к решению сравнений 1-й степени. Наилучшие приближения рациональными числами.	Составить программу Решение диофантовых уравнений с помощью. Цепных дробей. Самостоятельное изучение темы: Кольца Z_m с циклической группой обратимых элементов. Свойства индексов. Решение степенных сравнений	2,9	Текущий контроль Проверка программы
Итого по разделу		8,9	

Вопросы коллоквиумов

Тема: Простые числа. Делимость. Арифметические функции. Цепные дроби.

1. Понятие делимости. Свойства делимости.
2. Теорема о делении с остатком.

3. НОД двух и нескольких чисел. Алгоритм Евклида.
4. Основные свойства НОД двух и нескольких чисел.
5. НОК двух и нескольких чисел и его свойства. Связь НОД и НОК.
6. Простые числа. Критерий определения простоты числа.
7. Теорема Евклида о бесконечном множестве простых чисел. Разложение на простые множители.
8. Основная теорема арифметики. Каноническое разложение числа.
9. Решето Эратосфена.
10. Числовые функции. Функции $[x]$, $\{x\}$. Их свойства и графики. Теорема о вычислении показателя степени простого числа p в каноническом разложении $n!$
11. Мультипликативные функции и их свойства.
12. Суммы, распространенные на делители числа.
13. Функция Эйлера. Мультипликативность функции Эйлера. Формула для вычисления $\varphi(m)$.
14. Установление признаков делимости.
15. Определение длины периода, получающегося при обращении обыкновенной дроби в десятичную.
16. Разложение в правильную цепную дробь (конечную) рационального числа. Теорема о существовании и единственности значения цепной дроби для рационального числа.
17. Подходящие дроби конечных цепных дробей, их свойства.
18. Бесконечные цепные дроби. Разложение иррационального числа в бесконечную цепную дробь. Теоремы о том, что разложения иррациональных чисел исчерпывают все возможные бесконечные цепные дроби.
19. Подходящие дроби бесконечных цепных дробей, их свойства.
20. Теорема Лежандра о квадратичной иррациональности.

Тема: Теория сравнений.

1. Сравнения и их основные свойства.
2. Классы по данному модулю. Разбиение множества целых чисел на классы. Сложение и умножение классов. Кольцо классов.
3. Системы вычетов. Полная система вычетов. Признак полной системы вычетов.
4. Первая теорема о вычетах линейной формы.
5. Приведенная система вычетов. Признак приведенной системы вычетов.
6. Вторая теорема о вычетах линейной формы.
7. Теоремы Эйлера и Ферма.
8. Сравнения первой степени с неизвестной величиной. Критерий разрешимости и число решений. Решение методом подбора.
9. Решение сравнений первой степени при помощи теоремы Эйлера.
10. Системы сравнений первой степени. Общий случай. Случай попарно простых модулей.
11. Сравнения n -ой степени по простому модулю. Сведение к наиболее простому виду (теоремы о равносильности сравнений). Теорема о максимальном числе решений. Теорема Вильсона.
12. Сравнения по составному модулю: Приведение сравнения по составному модулю к системе сравнений по модулям попарно простым.
13. Общие сведения о двучленных сравнениях второй степени. Число решений.
14. Сравнения n -ой степени. Сравнения n -ой степени по простому модулю. Теоремы о равносильности сравнений. Теорема о числе решений сравнения. Теорема Вильсона.
15. Теорема о существовании и числе классов, принадлежащих показателю по простому модулю.
16. Теорема о существовании первообразного корня по простому модулю.
17. Применение индексов к решению сравнений. Критерий разрешимости двучленного сравнения по простому модулю.
18. Квадратичные вычеты. Число квадратичных вычетов. Критерий Эйлера.
19. Символ Лежандра. Свойства. Закон взаимности нечетных простых чисел.

Приложение 2

а) Планируемые результаты обучения и оценочные средства для проведения промежуточной аттестации:

Код индикатора	Индикатор достижения компетенции	Оценочные средства
ОПК-8 Способен осуществлять педагогическую деятельность на основе специальных научных знаний		
ОПК-8.1	Планирует и проводит научные исследования в области педагогической деятельности	Для осуществления научных исследований в области педагогической деятельности студент должен знать ответы на теоретические вопросы выводимые на зачет 1. Свойства делимости в кольце. Деление с остатком в кольце целых чисел. 2. Наибольший общий делитель. Алгоритм Евклида. Выражение наибольшего общего делителя (a,b) через a и b. 3. Наименьшее общее кратное. 4. Свойства взаимно простых чисел. 5. Факториальность кольца целых чисел (Основная теорема арифметики). Разложение на простые множители наибольшего общего делителя и наименьшего общего кратного. 6. Кольцо классов вычетов по модулю m. Свойства сравнений. Решение сравнений 1-степени. 7. Группа обратимых элементов кольца. Теорема Эйлера. Малая теорема Ферма. 8. Китайская теорема об остатках. Мультипликативность функции Эйлера. Вычисление функции Эйлера. 9. Формула Гаусса. 10. Китайская теорема об остатках. Решение системы сравнений по взаимно простым модулям. 11. Мультипликативные арифметические функции. Функция Мебиуса, формула обращения. 12. Конечные подгруппы в мультипликативной группе поля. Цикличность мультипликативной группы конечного поля. 13. Первообразные корни по модулю m. Индексы. 14. Квадратичные вычеты. Символ Лежандра и его свойства. 15. Лемма Гаусса. Символ Лежандра $(2/p)$. 16. Квадратичный закон взаимности. 17. Целая и дробная части числа. Кратность, с которой простое p входит в разложение $n!$ на простые множители. 18. Разложение рационального числа в цепную дробь с целыми неполными частными. Разложение вещественного числа в цепную дробь. 19. Подходящие дроби и их свойства. 20. Решение линейных уравнений в целых числах

Код индикатора	Индикатор достижения компетенции	Оценочные средства
		19. Бесконечные периодические цепные дроби и квадратичные иррациональности. 20. Приближение вещественных чисел рациональными числами и цепные дроби. 21. Закон распределения простых чисел Чебышева, асимптотический закон распределения простых чисел (без доказательства).
ОПК-8.2	Использует специальные научные знания для повышения эффективности педагогической деятельности	Студент должен уметь применять основные понятия, их свойства, формулы и теоремы при решении простых примеров и задач, применять основные понятия, их свойства, формулы и теоремы при решении примеров и задач средней сложности, входящие в школьный курс математики и используемые в других изучаемых предметах. Студент должен владеть навыками правильного выбора свойств, формул и теорем для решения простых задач и задач средней сложности
		Контрольная работа №1 Вариант 1. 1. Найти каноническое разложение числа C_{20}^{12} 2. Найти число делителей, сумму делителей и функцию Эйлера для числа 840.(ОПК-1) 3. Разложить в конечную цепную дробь число $\frac{162}{93}$, а затем вычислить все подходящие дроби. 4. Найти значение бесконечной периодической цепной дроби $\langle -1; 1, 1, (1, 2) \rangle$. 5. Разложить в периодическую цепную дробь число $\frac{\sqrt{3}-1}{2}$.
		Вариант 2. 1. Найти каноническое разложение числа $18!$ 2. Найти число делителей, сумму делителей и функцию Эйлера для числа 993. Разложить в конечную цепную дробь число $\frac{121}{88}$, а затем вычислить все подходящие дроби. 3. Найти значение бесконечной периодической цепной дроби $\langle 0, (1, 4, 1, 1) \rangle$. 4. Разложить в периодическую цепную дробь число

Код индикатора	Индикатор достижения компетенции	Оценочные средства
		$\frac{\sqrt{7}}{3}.$ Контрольная работа № 2 Теория делимости в кольце целых чисел. Основы теории цепных дробей ДЕМОНСТРАЦИОННЫЙ ВАРИАНТ - Запишите данные систематические дроби в виде обыкновенных в той же системе счисления: а) $0,87(102)_9$; б) $0,7(5)_8$. - Найдите наибольший общий делитель чисел 4081, 4972, 3377. - Представьте наибольший общий делитель чисел 646 и 976 в виде их линейной комбинации. - Найдите наименьшее общее кратное чисел 1910 и 1540. - Найдите каноническое разложение числа $125!$. - Разложите в цепную дробь и замените подходящей дробью с точностью до 0,001 число $\frac{2517}{773}$. - Найдите действительное число α, которое обращается в цепную дробь $[(1;3)]$. - Найдите все простые числа, для которых числа $p + 2$ и $p + 5$ одновременно являются простыми. Контрольная работа № 3 Теория сравнений. Теоретико-числовые методы в криптографии ДЕМОНСТРАЦИОННЫЙ ВАРИАНТ - Решите с помощью теоремы Эйлера сравнение $78x \equiv 30(\text{mod}198)$. - Решите с помощью цепных дробей сравнение $111x \equiv 147(\text{mod}87)$. - Решите систему сравнений $\begin{cases} x \equiv 2(\text{mod}5), \\ x \equiv 3(\text{mod}6), \\ x \equiv 4(\text{mod}7). \end{cases}$ - Найдите сравнение степени ниже 7, которому равносильно сравнение

Код индикатора	Индикатор достижения компетенции	Оценочные средства
		$2x^{11} + 5x^{10} + 2x^9 + 4x^8 + 2x^7 + 3x^6 + x^4 + 5x^3 + 3x^2 + 3x + 5 \equiv 0 \pmod{7}$. 5. Вычислите символ Лежандра $\left(\frac{88}{347} \right)$. 7. Проверьте результаты арифметических действий по модулю 9 и по модулю 11: а) $4237 \times 27925 = 111275855$; б) $\frac{42981}{8264} = 5201$.

Б) Показатели и критерии оценивания зачета (в соответствии с формируемыми компетенциями и планируемыми результатами обучения):

– на оценку «**зачтено**» – студент должен показать достаточный уровень знаний не только на уровне воспроизведения и объяснения информации, но и интеллектуальные навыки решения проблем и задач;

– на оценку «**не зачтено**» – студент не может показать знания на уровне воспроизведения и объяснения информации, не может показать интеллектуальные навыки решения простых задач.

Вопросы к зачету:

1. Понятие делимости. Свойства делимости.
2. Теорема о делении с остатком.
3. НОД двух и нескольких чисел. Алгоритм Евклида.
4. Основные свойства НОД двух и нескольких чисел.
5. НОК двух и нескольких чисел и его свойства. Связь НОД и НОК.
6. Простые числа. Критерий определения простоты числа.
7. Теорема Евклида о бесконечном множестве простых чисел. Разложение на простые множители.
8. Основная теорема арифметики. Каноническое разложение числа.
9. Мультипликативные функции и их свойства.
10. Суммы, распространенные на делители числа.
11. Функция Эйлера. Мультипликативность функции Эйлера. Формула для вычисления $\varphi(m)$.
12. Разложение в правильную цепную дробь (конечную) рационального числа. Теорема о существовании и единственности значения цепной дроби для рационального числа.
13. Подходящие дроби конечных цепных дробей, их свойства.

14. Бесконечные цепные дроби. Разложение иррационального числа в бесконечную цепную дробь. Теоремы о том, что разложения иррациональных чисел исчерпывают все возможные бесконечные цепные дроби.
15. Подходящие дроби бесконечных цепных дробей, их свойства.
16. Сравнения и их основные свойства.
17. Классы по данному модулю. Разбиение множества целых чисел на классы. Сложение и умножение классов. Кольцо классов.
18. Системы вычетов. Полная система вычетов. Признак полной системы вычетов.
19. Первая теорема о вычетах линейной формы.
20. Приведенная система вычетов. Признак приведенной системы вычетов.
21. Вторая теорема о вычетах линейной формы.
22. Теоремы Эйлера и Ферма.
23. Сравнения первой степени с неизвестной величиной. Критерий разрешимости и число решений. Решение методом подбора.
24. Решение сравнений первой степени при помощи теоремы Эйлера.
25. Системы сравнений первой степени. Общий случай. Случай попарно простых модулей.
26. Сравнения n -ой степени по простому модулю. Сведение к наиболее простому виду (теоремы о равносильности сравнений). Теорема о максимальном числе решений. Теорема Вильсона.
27. Сравнения по составному модулю: Приведение сравнения по составному модулю к системе сравнений по модулям попарно простым.