УТВЕРЖДАЮ
Проректор по учебной работе
_____ / В.Е. Федоров
«28» 08 2020 г.

Рабочая программа дисциплины (модуля)*
Теоретико-числовые методы в криптографии

Направление подготовки (специальность)

10.05.01 Компьютерная безопасность

Направленность (профиль)

специализация № 1 "Анализ безопасности компьютерных систем"

Присваиваемая квалификация (степень)

специалист по защите информации

Форма обучения

очная

Год(ы) набора 2018, 2019, 2020

*Рабочая программа дисциплины (модуля) адаптирована для инклюзивного обучения инвалидов и лиц с ограниченными возможностями здоровья

Челябинск 2020 г.

Рабочая программа дисциплины (модуля) принята:
Ученым советом математического факультета

Протокол заседания № 11 от «27» 08 2020 г.

Председатель Ученого совета
математического факультета _____ Е.А. Сбродова

Секретарь Ученого совета
математического факультета _____ С.А. Никитина

Рабочая программа дисциплины (модуля) одобрена и рекомендована кафедрой
компьютерной безопасности и прикладной алгебры

Протокол заседания № 13 от «27» июля 2020 г.

Заведующий кафедрой _____ А.Н. Ручай

Автор (составитель):
Д-р физ.мат.наук, профессор _____ В.В. Кораблева

Структура рабочей программы соответствует приказу ректора ФГБОУ ВО «ЧелГУ» от «05» декабря 2018 г. № 678-1

Содержание

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цель освоения учебной дисциплины состоит в овладении основными теоретико-числовыми методами, которые используются или могут использоваться в криптографии.

Задачами изучения дисциплины являются:

- изучение и освоение вероятностных и детерминистических алгоритмов простоты числа, алгоритмов факторизации числа, алгоритмов дискретного логарифмирования;

- овладение арифметическими операциями с большими целыми числами;

- изучение точных и асимптотических оценок сложности основных теоретико-числовых алгоритмов;

- ознакомление с современным состоянием алгоритмической теорией чисел.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Цикл (раздел) ОПОП: Б1.Б.1.35

2.1 Требования к предварительной подготовке обучающегося:

Освоение дисциплины опирается на знания по дисциплинам «Алгебра»,«Языки программирования», «Методы программирования», «Теория чисел».

Теория чисел

Языки программирования

Алгебра

Методы программирования

2.2 Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:

Дисциплина «Теоретико-числовые методы в криптографии» является предшествующей для дисциплин «Криптографические протоколы» и «Криптографические методы защиты информации».

Криптографические методы защиты информации

Криптографические протоколы

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

ОПК-2: способность корректно применять при решении профессиональных задач аппарат математического анализа, геометрии, алгебры, дискретной математики, математической логики, теории алгоритмов, теории вероятностей, математической статистики, теории информации, теоретике-числовых методов

Знать:

- точные и асимптотические оценки сложности основных теоретико-числовых алгоритмов;
- основные теоретико-числовые методы и подходы для решения прикладных задач.

Уметь:

- применять основные теоретико-числовые результаты, изучаемые в курсе, для решения задач в криптографии.

Владеть:

- основными теоретико-числовыми методами, которые используются или могут использоваться в криптографии.

В результате освоения дисциплины обучающийся должен

3.1	**Знать:**
3.1.1	- основные теоретико-числовые алгоритмы.
3.2	**Уметь:**
3.2.1	- проводить вычисления на эллиптических кривых, в конечных полях и с большими числами.
3.3	**Владеть:**
3.3.1	- владения методами вычисления с большими числами.

4. ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ)

Общая трудоемкость	**4 ЗЕТ**
Часов по учебному плану : 144 в том числе : аудиторные занятия : 54 самостоятельная работа : 72 часов на контроль : 18	Виды контроля в семестрах: экзамены 6

5. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Литература
	Раздел 1. 1. Оценка сложности арифметических операций			
1.1	Сложность арифметических операций с целыми числами. /Лек/	6	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1
1.2	Сложность арифметических операций с целыми числами. /Пр/	6	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1
1.3	Сложность арифметических операций с целыми числами. /Ср/	6	6	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1
1.4	Сложность арифметических операций в кольцах вычетов. /Лек/	6	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1
1.5	Сложность арифметических операций в кольцах вычетов. /Пр/	6	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1
1.6	Сложность арифметических операций в кольцах вычетов. /Ср/	6	6	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1
	Раздел 2. 2. Тестирование чисел на простоту и построение больших простых чисел			
2.1	Вероятностные тесты простоты (на основе малой теоремы Ферма, Рабина-Миллера, Соловея-Штрассена). /Лек/	6	4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1
2.2	Вероятностные тесты простоты (на основе малой теоремы Ферма, Рабина-Миллера, Соловея-Штрассена). /Пр/	6	1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1
2.3	Вероятностные тесты простоты (на основе малой теоремы Ферма, Рабина-Миллера, Соловея-Штрассена). /Ср/	6	6	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1
2.4	Алгоритм Конягина-Померанса. Алгоритм Миллера. /Лек/	6	4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1
2.5	Алгоритм Конягина-Померанса. Алгоритм Миллера. /Пр/	6	1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1
2.6	Алгоритм Конягина-Померанса. Алгоритм Миллера. /Ср/	6	6	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1
2.7	Современные методы проверки простоты числа. Детерминированный полиномиальный алгоритм проверки простоты чисел. /Лек/	6	4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1
2.8	Современные методы проверки простоты числа. Детерминированный полиномиальный алгоритм проверки простоты чисел. /Пр/	6	1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1
2.9	Современные методы проверки простоты числа. Детерминированный полиномиальный алгоритм проверки простоты чисел. /Ср/	6	6	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1
2.10	Тесты на простоту для чисел специального вида. Построение больших простых чисел. /Лек/	6	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1
2.11	Тесты на простоту для чисел специального вида. Построение больших простых чисел. /Пр/	6	1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1
2.12	Тесты на простоту для чисел специального вида. Построение больших простых чисел. /Ср/	6	6	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1

2.13	Тесты на простоту для чисел специального вида. Построение больших простых чисел. /Лек/	6	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1
2.14	Тесты на простоту для чисел специального вида. Построение больших простых чисел. /Пр/	6	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1
2.15	Тесты на простоту для чисел специального вида. Построение больших простых чисел. /Ср/	6	6	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1
	Раздел 3. 3. Факторизация целых чисел			
3.1	Экспоненциальные алгоритмы (метод пробных делений, Ро-метод Полларда, Ферма, (p-1)-метод Полларда, (p+1)-метод Вильямса, Шермана-Лемана, Ленстры). /Лек/	6	6	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1
3.2	Экспоненциальные алгоритмы (метод пробных делений, Ро-метод Полларда, Ферма, (p-1)-метод Полларда, (p+1)-метод Вильямса, Шермана-Лемана, Ленстры). /Пр/	6	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1
3.3	Экспоненциальные алгоритмы (метод пробных делений, Ро-метод Полларда, Ферма, (p-1)-метод Полларда, (p+1)-метод Вильямса, Шермана-Лемана, Ленстры). /Ср/	6	10	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1
3.4	Субэкспоненциальные алгоритмы Диксона, Бриллхарта-Моррисона, метод решета). /Лек/	6	6	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1
3.5	Субэкспоненциальные алгоритмы Диксона, Бриллхарта-Моррисона, метод решета). /Пр/	6	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1
3.6	Субэкспоненциальные алгоритмы Диксона, Бриллхарта-Моррисона, метод решета). /Ср/	6	10	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1
3.7	Применение эллиптических кривых для проверки простоты и факторизации. /Лек/	6	4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1
3.8	Применение эллиптических кривых для проверки простоты и факторизации. /Пр/	6	4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1
3.9	Применение эллиптических кривых для проверки простоты и факторизации. /Ср/	6	10	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1
	Раздел 4. Экзамен			
4.1	/Экзамен/	6	18	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

6.1. Перечень видов оценочных средств

Контрольная работа.
Коллоквиум.
Экзамен.

6.2. Типовые контрольные задания и иные материалы для текущей аттестации

Перечень вопросов к коллоквиуму

1. Тест на основе теоремы Ферма.
2. Свойства псевдопростых чисел.
3. Свойства чисел Кармайкла (доказать).
4. Тест Соловея-Штрассена, его обоснование.
5. Тест Рабина –Миллера, его обоснование.
6. Тесты на простоту для чисел специального вида.
7. Алгоритм Конягина-Померанса.
8. Алгоритм Ферма (факторизация).
9. ρ- метод Полларда (факторизация).
10. Алгоритм Ленстры (факторизация).

11. Алгоритм Шермана-Лемана (факторизация).
12. Алгоритм Диксона (факторизация).
13. Алгоритм Миллера (детерминированный).
14. Алгоритм ПоллардаШтрассена (факторизация).
15. $P+1$ метод Вильямса (факторизация).

6.3. Типовые контрольные вопросы и задания для промежуточной аттестации

Перечень вопросов к экзамену
1. Решето Эратосфена.
2. Критерий Вильсона.
3. Тест на основе теоремы Ферма.
4. Свойства псевдопростых чисел (доказать).
5. Свойства чисел Кармайкла (доказать).
6. Тест Соловея-Штрассена, его обоснование.
7. Тест Рабина –Миллера, его обоснование.
8. Тесты на простоту для чисел специального вида.
9. Алгоритм Конягина-Померанса.
10. Алгоритм Ферма (факторизация).
11. ρ- метод Полларда (факторизация).
12. Алгоритм Ленстры (факторизация).
13. Алгоритм Шермана-Лемана (факторизация).
14. Алгоритм Диксона (факторизация).
15. Алгоритм Миллера (детерминированный).
16. Алгоритм Берлекэмпа.
17. Алгоритм ПоллардаШтрассена (факторизация).
18. $P+1$ метод Уильямса (факторизация).
19. Квадратичное решето.

6.4. Критерии оценивания

Балльно-рейтинговая система оценки знаний студента по дисциплине выстраивается на основе балловой оценки различных форм деятельности студентов. Для оценки экзамена суммируются баллы семестра и экзамена.

Фонд оценочных средств представляет собой комплекс контрольных работ, вопросы к коллоквиуму и экзаменационные билеты, которые позволяют оценить регулярную работу студента, направленную на формирование компетенций и достижение планируемых результатов обучения.
В ходе изучения дисциплины «Теоретико-числовые методы в криптографии» студент должен выполнить 2 контрольные работы и сдать 1 коллоквиум. Каждая из контрольных работ и коллоквиум оценивается в 20 баллов. В конце семестра сдаётся экзамен Нарушение срока выполнения контрольной работы и сдачи коллоквиума без уважительной причины ведет за собой снижение баллов за контрольную работу и коллоквиум на 2 балла за каждую неделю задержки.

Билеты для экзамена содержат 4 задания (2 практических задачи и 2 теоретических вопроса). За каждое выполненное задание билета студент может получить от 2 до 5 баллов.
Если задание выполнено правильно, то оно оценивается 5 баллами.
Если задание выполнено с ошибками, то баллы снижаются в зависимости от количества допущенных ошибок.
Если допущена одна ошибка, то здание оценивается 4 баллами, допущены две ошибки – 3 баллами, допущены три ошибки – 2 баллами.
Если задание выполнено частично, и выполненная часть задания не содержит ошибок, то оно оценивается 2 баллами.
Если допущено более трех ошибок в задании или студент выполнил менее трети задания из билета, то за него он получает 0 баллов.

Наименование оценочного средства Максимальное кол-во баллов
Билет для экзамена 20
Контрольная работ (Коллоквиум) 20

Согласно положению о БРС, окончательная оценка на экзамене выставляется с учетом баллов, полученных студентом в течение семестра. Итоговая оценка складывается из суммы баллов полученных за работу в семестре и за ответ на экзамене.

В течение учебного семестра студенты за каждый вид работы получают баллы. Итоговая оценка в семестре складывается из суммы баллов, полученных в семестре, и за ответ на экзамене. Затем полученная сумма баллов переводится в оценку, согласно положению о БРС. При этом допускается получение студентом автоматической оценки только по результатам работы в семестре.

Сводная таблица рейтинга успеваемости

№	Перечень контрольных мероприятий в семестре	Максимальное кол-во баллов
1	Контрольные работы (коллоквиум)	60
2	Активная работа на занятиях в течение семестра	10
3	Посещаемость (все занятия)	5
4	Выполнение всех домашних заданий	5
5	Ответ на экзамене	20
Итого		100

Критерии оценивания экзамена:

№ п/п	Набранные баллы	Оценка
1	Менее 50	неудовлетворительно
2	50 – 69	удовлетворительно
3	70 – 90	хорошо
4	91 – 100	отлично

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

7.1. Рекомендуемая литература

7.1.1. Основная литература

	Авторы, составители	Заглавие	Издательство, год	Ресурс
Л1.1	Василенко О. Н.	Теоретико-числовые алгоритмы в криптографии (2-е издание, дополненное): монография (http://biblioclub.ru/index.php?page=book&id=61814)	Москва : МЦНМО, 2006	ЭБС
Л1.2	Кнауб Л. В., Новиков Е. А., Шитов Ю. А.	Теоретико-численные методы в криптографии: учебное пособие (http://biblioclub.ru/index.php?page=book&id=229582)	Красноярск : Сибирский федеральный университет (СФУ), 2011	ЭБС
Л1.3		Теоретико-числовые методы в криптографии: практикум (http://biblioclub.ru/index.php?page=book&id=483838)	Ставрополь : Северо-Кавказский Федеральный университет (СКФУ), 2017	ЭБС

7.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год	Ресурс
Л2.1	Глухов М. М., Круглов И. А.	Элементы теории обыкновенных представлений и характеров конечных групп с приложениями в криптографии (http://e.lanbook.com/books/element.php?pl1_id=65044)	Санкт- Петербург : Лань, 2015	ЭБС
Л2.2	Глухов М. М., Круглов И. А., Пичкур А. Б., Черемушкин А. В.	Введение в теоретико-числовые методы криптографии: учебное пособие для вузов	Санкт-Петербург [и др.]: Лань, 2011	
Л2.3	Болелов Э.А.	Информационный мир XXI века. Криптография- основа информационной безопасности: учебно-методическая литература (http://znanium.com/catalog/document?id=353538)	Москва : Дашков и К, 2020	ЭБС

7.1.3. Методические разработки

	Авторы, составители	Заглавие	Издательство, год	Ресурс
Л3.1	Ниссенбаум О. В.	Теоретико-числовые методы в криптографии. Сборник заданий: учебно-методическое пособие для студентов специальностей «Компьютерная безопасность» и «Информационная безопасность автоматизированных систем», направления «Информационная безопасность»: учебно-методическое пособие (http://biblioclub.ru/index.php?page=book&id=567498)	Тюмень : Тюменский государственный университет, 2014	ЭБС

7.3 Перечень информационных технологий

7.3.1 Программное обеспечение

Visual Studio

Python

Notepad++

WinDjView

Java Development Kit

Adobe Reader

7.3.2 Профессиональные базы данных и информационно-справочные системы

1. Электронный каталог научной библиотеки ЧелГУ [Электронный ресурс] : база данных / Челяб. гос. ун-т. – Челябинск, 1992.

2. Консультант Плюс [Электронный ресурс] : справочно-правовая система : база данных / Регион. центр правовой информ. Информправо.

3. eLIBRARY.RU [Электронный ресурс] : научная электронная библиотека [научной периодики на русском языке]. — Москва, [1999-]. - Доступ к полным текстам после регистрации из сети ЧелГУ. – URL: http://elibrary.ru/defaultx.asp.

4. Moodle [Электронный ресурс]: система дистанционного обучения : [база данных] / Челяб. гос. ун-т. – Челябинск, [б.г.]. – Доступ из сети ЧелГУ или, после регистрации из сети ун-та, из любой точки, имеющей доступ в интернет. – URL: http://moodle.uio.csu.ru/login/index.php.

5. Научная библиотека Челябинского государственного университета [Электронный ресурс] : [сайт] / Челяб. гос. ун-т. – Челябинск, [2001-]. – Режим доступа: http://www.lib.csu.ru/ , свободный. – Загл. с экрана.

6. Интернет университет информационных технологий [Электронный ресурс]. – Электрон. дан. – Режим доступа : http://www.intuit.ru/

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Для реализации дисциплины используются учебные аудитории для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы.

Учебные аудитории укомплектованы специализированной мебелью и техническими средствами обучения: проектором, экраном, магнитно-маркерной доской, маркером; с возможностью демонстрации электронных презентаций при уровне освещения, достаточном для работы с конспектом.

Для проведения занятий лекционного типа имеется демонстрационное оборудование: проектор, экран.

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

9. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

При изучении данной дисциплины используются лекционные, практические занятия и самостоятельная работа студента. На лекционных занятиях преподаватель излагает основное содержание тем программы. Проработку лекционного материала студенту желательно проводить как после каждого занятия, так и по завершению темы. Это позволит связать воедино полученные сведения и составить цельную картину.
На практических занятиях рассматриваются конкретные способы реализации теоретико-числовых алгоритмов.
Рекомендуется перед каждым практическим занятием выполнить домашнее задание, что позволить лучше усвоить предыдущий материал, и изучить лекционный материал по предстоящей теме. Студенту желательно проявлять активное участие на практических и лекционных занятиях, задавать вопросы, поскольку умение обосновывать свою точку зрения, нахождение компромиссного решения в этически выдержанной дискуссии не только важно для лучшего усвоения материала, но и ценится в реальной жизни.

В случае применения при обучении дисциплины электронного обучения, дистанционных образовательных технологий общение обучающихся и преподавателя осуществляется в режиме реального времени (онлайн-лекции (вебинары), чаты, видео-конференции и др.) или отложенного времени (система дистанционного обучения Moodle, видеохостинг YouYube, форумы, электронная почта и др.).
Большую часть времени обучающиеся самостоятельно работают с учебно-методическими материалами. Студенты имеют возможность консультироваться с преподавателем по всем вопросам, возникающим в ходе самостоятельной работы посредством электронной почты, мессенджеров, социальных сетей и т.п.
Доступ обучающегося к учебным ресурсам в режиме отложенного времени, самостоятельной работы осуществляется через сеть Интернет в удобном для него месте, времени и темпе.

При обучении лиц с ограниченными возможностями здоровья электронное обучение, дистанционные образовательные технологии предусматривают возможность приема-передачи информации в доступных для них формах.
Реализация дисциплины с применением электронного обучения, дистанционных образовательных технологий (далее – ЭО, ДОТ) осуществляется на основании «Положения о реализации основных и дополнительных образовательных программ с применением электронного обучения и дистанционных образовательных технологий в федеральном государственном бюджетном образовательном учреждении высшего образования «Челябинский государственный

университет», «Положения о порядке зачета обучающимися по основным профессиональным образовательным программам высшего образования в ФГБОУ ВО «ЧелГУ» результатов освоения в организациях, осуществляющих образовательную деятельность, учебных предметов, курсов, дисциплин (модулей), практик, дополнительных образовательных программ» посредством электронной информационно-образовательной среды ФГБОУ ВО «ЧелГУ». В исключительных случаях (форс-мажор и т.п.) при реализации образовательной деятельности с применением ЭО, ДОТ могут применять компоненты, не входящие в перечень электронной информационно-образовательной среды.

10. СПЕЦИАЛЬНЫЕ УСЛОВИЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ ОБУЧАЮЩИМИСЯ С ИНВАЛИДНОСТЬЮ И ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

Освоение дисциплины инвалидами и лицами с ограниченными возможностями здоровья осуществляется с использованием специальных технических средств и голо информационных технологий, предоставляемых Ресурсным учебно-методическим центром по обучению инвалидов и лиц с ограниченными возможностями здоровья ЧелГУ по запросу обучающегося.

1. Мобильные специальные технические средства для лиц с нарушениями зрения: портативный компьютер с вводом/выводом шрифтом Брайля с синтезатором речи «ElBraile-W14J G2»; ноутбуки с программной экранного доступа NVDA; электронные увеличители для удаленного просмотра; видеоувеличители портативные; тифлоплеер; цифровые диктофоны.

2. Мобильные специальные технические средства для лиц с нарушениями слуха: система свободного звукового поля со встроенной совместимостью с FM-устройствами; радиоклассы «Сонет-РСМ» с передатчиком, заушным индуктором и индукционной петлей; система информационная для слабослышащих переносная «Исток» А2 со встроенным плеером – звуковым информатором; документ-камера; программируемые слуховые аппараты индивидуального пользования.

3. Ассистивные информационные технологии: программное обеспечение экранного доступа с синтезом речи NVDA; программы экранного увеличения; программы речевого синтеза для компьютеров и ноутбуков; программы речевого синтеза для мобильных устройств; экранная клавиатура; экранная лупа.

При необходимости для обучающихся с нарушениями зрения на рабочих местах для проведения практических или лабораторных занятий устанавливается специальное программное обеспечение (программа речевой навигации NVDA, речевые синтезаторы, экранные лупы).

В учебные аудитории обеспечивается беспрепятственный доступ для обучающихся инвалидов и обучающихся с ограниченными возможностями здоровья. В каждой аудитории, где обучаются инвалиды и лица с ограниченными возможностями здоровья, предусматривается соответствующее количество мест для обучающихся с учетом нарушений их здоровья.

Для освоения дисциплины инвалидам и лицам с ограниченными возможностями здоровья предоставляется доступ к печатным источникам, имеющимся в научной библиотеке ЧелГУ, с помощью специальных технических средств; доступ к электронным источникам, представленным в форме электронного документа в фонде научной библиотеки ЧелГУ или электронно-библиотечных системах, с помощью специальных технических и программных средств (рабочее место для незрячего пользователя с программным обеспечением экранного доступа с синтезом речи NVDA, рабочее место с компьютерным роллером и клавиатурой Clevy с большими кнопками и с разделяющей клавиши накладкой).

Учебно-методические материалы для обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:
- в печатной форме увеличенным шрифтом,
- в форме электронного документа,
- в форме аудиофайла,
- в печатной форме шрифтом Брайля.

Для лиц с нарушениями слуха:
- в печатной форме,
- в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:
- в печатной форме,
- в форме электронного документа,
- в форме аудиофайла.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

Для инвалидов и лиц с ограниченными возможностями здоровья освоение дисциплины может быть частично или полностью осуществлено с использованием дистанционных образовательных технологий (Moodle, Adobe Connect Pro и пр.).

В освоении дисциплины инвалидами и лицами с ограниченными возможностями здоровья используется индивидуальная работа. Под индивидуальной работой подразумевается две формы взаимодействия с преподавателем: индивидуальная учебная работа (консультации), т.е. дополнительное разъяснение учебного материала и углубленное изучение материала с теми обучающимися, которые в этом заинтересованы, и индивидуальная воспитательная работа. Индивидуальные консультации направлены на индивидуализацию обучения

и установлению воспитательного контакта между преподавателем и обучающимся инвалидом или обучающимся с ограниченными возможностями здоровья.

При проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине обеспечивается выполнение следующих дополнительных требований в зависимости от индивидуальных особенностей, обучающихся:

а) инструкция по порядку проведения процедуры оценивания предоставляется в доступной форме (устно, в письменной форме, в письменной форме шрифтом Брайля, устно с использованием услуг сурдопереводчика);

б) доступная форма предоставления заданий оценочных средств (в печатной форме, в печатной форме увеличенным шрифтом, в печатной форме шрифтом Брайля, в форме электронного документа, задания зачитываются ассистентом, задания предоставляются с использованием сурдоперевода);

в) доступная форма предоставления ответов на задания (письменно на бумаге, набор ответов на компьютере, письменно шрифтом Брайля, с использованием услуг ассистента, устно).

При проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья предусматривается использование технических средств, необходимых им в связи с их индивидуальными особенностями. Эти средства могут быть предоставлены ЧелГУ или могут использоваться собственные технические средства. При необходимости инвалидам и лицам с ограниченными возможностями здоровья предоставляется дополнительное время для подготовки ответа на задания, процедура оценивания результатов обучения по дисциплине может проводиться в несколько этапов.

Проведение процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья допускается с использованием дистанционных образовательных технологий.

Задание для самостоятельной подготовки к экзамену.

1. Доказать, что если n — псевдопростое по основанию 2, то $N = 2^n - 1$ является сильно псевдопростым и эйлеровым псевдопростым по основанию2.

2. Доказать, что существует бесконечно много псевдопростых и эйлеровых псевдопростых по основанию 2.

3. Найти все основания b, для которых 15 — псевдопростое число (не включать тривиальные основания ± 1).

4. Найти все основания, для которых 21 — псевдопростое число.

5. Доказать, что существует 36 оснований $b \in (\mathbb{Z}/91\mathbb{Z})^*$ (т.е. половина всех возможных оснований), для которых 91 — псевдопростое число.

6. Показать, что если p и $2p-1$ — простые числа и $n = p(2p-1)$, то n — псевдопростое для 50% возможных оснований b, а именно, для тех b, которые являются квадратичными вычетами по модулю $2p - 1$.

7. Доказать, что никакое целое число $n = 3p$ ($p > 3$ есть простое число) не может быть псевдопростым по основаниям $2, 5$ или 7.

8. Доказать, что никакое целое $n = 5p$ ($p > 5$ есть простое число) не может быть псевдопростым по основаниям $2, 3$ или 7.

9. Доказать, что 91 — наименьшее псевдопростое число по основанию 3.

10. Найти наименьшее псевдопростое по основанию 5.

11. Найти наименьшее псевдопростое по основанию 2.

12. Доказать, что если n — псевдопростое по основанию 2, то $N = 2^n - 1$ — также псевдопростое по тому же основанию.

13. Доказать, что если n — псевдопростое по основанию b и НОД$(b-1, n) = 1$, то целое число $N = \dfrac{b^n - 1}{b - 1}$ — псевдопростое по основанию b.

14. Доказать, что существует бесконечно много псевдопростых чисел по основаниям 2, 3, 5.

15. Привести пример, показывающий, что если n — псевдопростое по основанию b, то целое число $N = \dfrac{b^n - 1}{b - 1}$ — псевдопростое по основанию b — неверно.

КОНТРОЛЬНОЕ ЗАДАНИЕ

1. Найти наибольший общий делитель и наименьшее общее кратное чисел 1) 252 и 468; 2) 279 и 372; 3) 178 и 381; 4) 318 и 477; 5) 758 и 1137; 6) 187 и 533; 7) 360 и 504.

2. Найти сумму делителей и число делителей чисел 1) 4320; 2) 1890; 3) 1500; 4) 1440; 5) 1200; 6) 990; 7) 998.

3. Найти значение функции Эйлера для чисел 1) 4320; 2) 1890; 3) 1500; 4) 1440; 5) 1200; 6) 990; 7) 998.

4. Найти остатки от деления 1) 383^{175} на 45; 2) 109^{345} на 14; 3) 439^{291} на 60; 4) 293^{275} на 48; 5) $5^{70}+7^{50}$ на 12; 6) $5^{50}+13^{100}$ на 18; 7) 243^{432} на 1000.

5. Решить сравнения 1) $114x \equiv 42(87)$; 2) $78x \equiv 42(51)$; 3) $14x \equiv 22(36)$; 4) $375x \equiv 195(501)$; 5) $90x \equiv -18(138)$; 6) $39x \equiv 84(93)$; 7) $10x \equiv 25(35)$.

6. Решить системы сравнений 1) $\begin{cases} 3x \equiv 1(10) \\ 4x \equiv 3(5) \\ 2x \equiv 7(9); \end{cases}$ 2) $\begin{cases} 5x \equiv 1(12) \\ 5x \equiv 2(8) \\ 7x \equiv 3(11); \end{cases}$ 3) $\begin{cases} 4x \equiv 1(9) \\ 5x \equiv 3(7) \\ 4x \equiv 5(12); \end{cases}$

4) $\begin{cases} 3x \equiv 7(10) \\ 2x \equiv 5(16) \\ 7x \equiv 5(12); \end{cases}$ 5) $\begin{cases} 4x \equiv 1(13) \\ 8x \equiv 16(17) \\ 8x \equiv 4(14); \end{cases}$ 6) $\begin{cases} 4x \equiv 14(26) \\ 5x \equiv 8(17) \\ 3x \equiv 7(31); \end{cases}$ 7) $\begin{cases} 4x \equiv 1(7) \\ 10x \equiv 6(22) \\ 11x \equiv 7(13). \end{cases}$

7. Решить в целых числах уравнения 1) $43x+37y=21$; 2) $53x+47y=11$; 3) $45x-37y=25$; 4) $81x-48y=33$; 5) $26x+34y=13$; 6) $122x+129y=21$; 7) $258x-172y=56$.

8. Решить сравнения, понизив их степени 1) $x^7-x^6+5x^2-3 \equiv 0(5)$; 2) $x^5+x^4+x^3-x^2-2 \equiv 0(5)$; 3) $x^7-6 \equiv 0(5)$; 4) $x^8+2x^7+x^5-x^4-x+3 \equiv 0(5)$; 5) $6x^4+17x^2-16 \equiv 0(3)$; 6) $4x^7-2x^3+84 \equiv 0(5)$; 7) $3x^7-2x^6+2x^2+13 \equiv 0(5)$.

9. Решить сравнения по составным модулям 1) $x^5-5x^4-5x^3+25x^2+4x-20 \equiv 0(147)$; 2) $x^5+3x^4-7x^3+4x^2+4x-10 \equiv 0(175)$; 3) $x^4-4x^3+2x^2+x+6 \equiv 0(135)$; 4) $4x^3+7x^2-7x-10 \equiv 0(225)$; 5) $31x^4+57x^3+96x+191 \equiv 0(225)$; 6) $2x^6-6x^4-7x^2-4 \equiv 0(441)$; 7) $2x^6-6x^4-7x^2-4 \equiv 0(1225)$.

10. Найти символы Лежандра 1) $\left(\frac{35}{97}\right)$; 2) $\left(\frac{47}{73}\right)$; 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) $\left(\frac{342}{677}\right)$.

11. Найти все первообразные корни по модулям 1)11, 2) 7, 3) 13, 4) 17, 5)10, 6) 14, 7) 22.

12. Найти показатель x в сравнениях 1) $2^x \equiv 7(67)$; 2) $13^x \equiv 12(47)$; 3) $16^x \equiv 11(53)$; 4) $52^x \equiv 38(61)$; 5) $12^x \equiv 17(31)$; 6) $20^x \equiv 21(41)$; 7) $23^x \equiv 7(41)$.

13. Разложить обыкновенную дробь в непрерывную (цепную) 1) $\frac{3587}{2743}$; 2) $\frac{1043}{3427}$; 3) $\frac{3653}{3107}$; 4) $\frac{11281}{6583}$; 5) $\frac{11111}{7093}$; 6) $\frac{2341}{1721}$; 7) $\frac{1882}{1721}$.

14. Найти третью подходящую дробь для 1) $\sqrt{11}$; 2) $\sqrt{10}$; 3) $\sqrt{12}$; 4) $1+\sqrt{5}$; 5) $1+\sqrt{7}$; 6) $1+\sqrt{2}$; 7) $1+\sqrt{3}$.