Министерство науки и высшего образования Российской Федерации
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ (НИ ТГУ)

Механико-математический факультет

УТВЕРЖДАЮ:
Декан
_____Л. В.Гензе
«20» 06 2022 г.

Рабочая программа дисциплины

Избранные вопросы теории чисел

по направлению подготовки

01.04.01 Математика

Направленность (профиль) подготовки :
Фундаментальная математика

Форма обучения
Очная

Квалификация
Магистр

Год приема
2022

Код дисциплины в учебном плане: Б1.В.2.ДВ.02.01

СОГЛАСОВАНО:
Руководитель ОП
_____П.А.Крылов

Председатель УМК
_____Е.А.Тарасов

Томск – 2022

1. Цель и планируемые результаты освоения дисциплины

Целью освоения дисциплины является формирование следующих компетенций:

ОПК-1 Способен формулировать и решать актуальные и значимые проблемы математики.

Результатами освоения дисциплины являются следующие индикаторы достижения компетенций:

ИОПК 1.1 Формулирует поставленную задачу, пользуется языком предметной области, обоснованно выбирает метод решения задачи.

2. Задачи освоения дисциплины

– Освоить аппарат дисциплины и получить прочные теоретические знания и практические навыки для возможности дальнейшего развития теоретико-числовых алгоритмов.

– Научиться применять понятийный аппарат теоретико-числовых алгоритмов для решения практических задач профессиональной деятельности, в том числе криптографии и криптоанализе.

3. Место дисциплины в структуре образовательной программы

Дисциплина относится к Блоку 1 «Дисциплина (модули)».

Дисциплина относится к части образовательной программы, формируемой участниками образовательных отношений, предлагается обучающимся на выбор.

4. Семестр(ы) освоения и форма(ы) промежуточной аттестации по дисциплине

Третий семестр, экзамен

5. Входные требования для освоения дисциплины

Для успешного освоения дисциплины требуются результаты обучения по следующим дисциплинам: «Теория чисел», «Алгебра», «Математический анализ».

6. Язык реализации

Русский

7. Объем дисциплины

Общая трудоемкость дисциплины составляет 4 з.е., 144 часов, из которых:
-лекции: 32 ч.
в том числе практическая подготовка: 0 ч.
Объем самостоятельной работы студента определен учебным планом.

8. Содержание дисциплины, структурированное по темам

Тема 1. *Алгоритмы приведения чисел по модулю.*
Алгоритм Баррета. Нахождение обратного элемента в кольцах вычетов.
Тема 2. *Алгоритмы быстрого возведения в степень.*
Алгоритм быстрого возведения в квадрат. Бинарный алгоритм.
Тема 3. *Дискретное преобразование Фурье.*
Примитивные корни. Остаток от деления многочленов.
Тема 4. *Алгоритм Монтгомери.*
Умножение по Монтгомери. Возведение в степень

Тема 5. *Нахождение корней многочленов в кольцах вычетов.*

Случай простого модуля. Случай степенного модуля.

Тема 6. *Извлечение корня в кольцах вычетов.*

Алгоритм Чипполы. Случаи четной и нечетной степени.

Тема 7. *Показательные сравнения.*

Случаи четного и нечетного модуля.

Тема 8. *Проверка простоты целых чисел.*

Тест Соловея-Штрассена. Числа Кармайкла. Тест Миллера-Рабина. Алгоритм Люка-Лемера. Полиномиальный тест.

Тема 9. *Построение больших простых чисел.*

Тесты на основе теоремы Поклингтона. Алгоритм Маурера. Сильно простые числа. Алгоритм Гордона.

Тема 10. *Алгоритмы факторизации.*

ρ-Метод Полларда. Метод Ферма. (*p*-1)-Метод Полларда. Алгоритм Диксона. Алгоритм Бриллхарта-Моррисона. Метод квадратичного решета.

Тема 11. *Вычисление дискретных логарифмов.*

Алгоритм Гельфонда-Шэнкса. Метод сведения к собственным подгруппам. Метод Сильвера-Полига-Хеллмана.

9. Текущий контроль по дисциплине

Текущий контроль по дисциплине проводится путем контроля посещаемости, проведения контрольных работ, тестов по лекционному материалу, деловых игр по темам, выполнения домашних заданий, и фиксируется в форме контрольной точки не менее одного раза в семестр.

10. Порядок проведения и критерии оценивания промежуточной аттестации

Экзамен в третьем семестре проводится в письменной форме по билетам. Экзаменационный билет состоит из трех частей. Продолжительность экзамена 1,5 часа.

Примерный перечень теоретических вопросов первой части.

Вопрос. Алгоритм Монтгомери относится к алгоритмам:

а) нахождения первообразных корней по модулю;

б) модульной арифметики;

в) проверки простоты натуральных чисел;

г) факторизации;

д) дискретного логарифмирования.

Примерный перечень теоретических вопросов второй части.

Вопрос 1. Доказать теорему Поклингтона о виде простых делителей числа N, для которого известно частичное разложение на множители числа N-1.

Вопрос 2. Обосновать принципиальное отличие теста Миллера-Рабина проверки простоты числа от теста Соловея-Штрассена.

Вопрос 3. Докажите, что множество вычетов по модулю N, относительно которых N является эйлеровым псевдопростым, образует подгруппу.

Примерный перечень задач из третьей части. Решение при помощи инженерного калькулятора.

Задача 1. При помощи алгоритма Чипполы найти квадратный корень из a по модулю p, если $p = 19$, $a = 13$.

Задача 2. Решить сравнение $x^7 = -88 \bmod 841$.

Задача 3. Решить сравнение $11^x = 19 \bmod 529$.

Результаты экзамена определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Инд. задание в системе Moodle.	20%	В течение семестра	По 100 бальной системе.
Тесты в системе Moodle.	20%	В течение семестра	Максимальное использование возможностей программы
Экзамен	60%	В конце семестра	Студент допускается до экзамена только при наличии выполненных индивидуального задания и теста. 1) Полный ответ, изложенный кратко и ясно – «отлично». 2) Ответ неполный (но > 70%), пояснения логически непротиворечивы – «хорошо». 3) Ответ неполный (но >50%), отсутствие логики в пояснениях – «удовлетворительно». 4) Ответ неполный (<50%), отсутствие логики в пояснениях или по сути отсутствует – «неудовлетворительно».

11. Учебно-методическое обеспечение

а) Электронный учебный курс по дисциплине в электронном университете «Moodle» - https://moodle.tsu.ru/course/view.php?id=25414

б) Оценочные материалы текущего контроля и промежуточной аттестации по дисциплине.

в) План семинарских / практических занятий по дисциплине.

Содержание дисциплины						
Темы занятий	**Контактные часы**				**Самостоятельная работа**	
	Лекции	Практические занятия	Лабораторные занятия	Консультации	Часы СРС	Задания
1. Алгоритмы приведения чисел по модулю.	2					
2. Алгоритмы быстрого возведения в степень.	2					
3. Дискретное преобразование Фурье.	3					
4. Алгоритм Монтгомери.	3					
5. Нахождение корней многочленов в кольцах вычетов	3					
6. Извлечение корня в кольцах вычетов	3					
7. Показательные сравнения.	3					
8. Проверка простоты целых чисел.	3					
9. Построение больших простых чисел.	3					
10. Алгоритмы факторизации	3					
11. Вычисление дискретных логарифмов	4					
Всего (без консультаций)	32					

г) Методические указания по проведению лабораторных работ.

Полностью и своевременно выполнять домашние задания и тесты. Для контроля следует использовать материалы лекций и семинарских занятий.

д) Методические указания по организации самостоятельной работы студентов.

Чтение основной литературы, указанной в нижеприводимом списке. Для контроля усвоения материала следует самостоятельно повторять доказательства основных теорем курса, а также решать задачи и упражнения, указанные в литературе, использовать электронные ресурсы.

12. Перечень учебной литературы и ресурсов сети Интернет

а) основная литература:

1. Глухов М.М., Круглов И.А., Пичкур А.Б., Черемушкин А. В. Введение в теоретико-числовые методы криптографии. СПб. Лань, 2021. 400 с.
2. Маховенко Е. Б. Теоретико-числовые методы в криптографии. М.: Гелиос АРВ, 2006. 320 с.
3. Черемушкин А.В. Лекции по арифметическим алгоритмам в криптографии. М.: МЦНМО, 2002. 104 с.

б) дополнительная литература:

1. Василенко О. Н. Теоретико-числовые алгоритмы в криптографии. М.: МЦНМО, 2-е изд. 2007. 336 с.
2. Манин Ю. И., Панчишкин А.А. Введение в современную теорию чисел. М.: МЦНМО, 2013. 552 с.
3. Авдошин С. Дискретная математика. Модулярная алгебра, криптография, кодирование. Москва: СИНТЕГ, 2016. - 260 с.
4. Арнольд И.В. Теория чисел. М.: Ленанд, 2019. – 288 с.
5. Боревич З.И., Шафаревич И.Р. Теория чисел. М.: Ленанд, 2019. – 504 с.
6. Панкратова И. А. Теоретико-числовые методы в криптографии. Томск, 2009. 120 с.

в) ресурсы сети Интернет, открытые онлайн-курсы:

– https://stepik.org/course/87474/promo
– https://www.youtube.com/playlist?list=PL-_cKNuVAYAW9WQYuzKGIdnlQTbo3x33G
– https://academiait.ru/course/algoritmy/
– https://romansementsov.ru/Курсы_Алгоритмы_Данных/
– сайт журнала «Вестник Томского государственного университета. Математика и механика» http://journals.tsu.ru/mathematics/

13. Перечень информационных технологий

а) лицензионное и свободно распространяемое программное обеспечение:

– Microsoft Office Standart 2013 Russian: пакет программ. Включает приложения: MS Office Word, MS Office Excel, MS Office PowerPoint, MS Office On-eNote, MS Office Publisher, MS Outlook, MS Office Web Apps (Word Excel MS PowerPoint Outlook);
– публично доступные облачные технологии (Google Docs, Яндекс диск и т.п.).

б) информационные справочные системы:

– Электронный каталог Научной библиотеки ТГУ – http://chamo.lib.tsu.ru/search/query?locale=ru&theme=system
– Электронная библиотека (репозиторий) ТГУ – http://vital.lib.tsu.ru/vital/access/manager/Index

– ЭБС Лань – http://e.lanbook.com/
– ЭБС Консультант студента – http://www.studentlibrary.ru/

в) профессиональные базы данных:
– Web of Science https://lib.tusur.ru/ru/resursy/bazy-dannyh/web-of-science
– Scopus https://lib.tusur.ru/ru/resursy/bazy-dannyh/scopus
– zbMATH https://lib.tusur.ru/ru/resursy/bazy-dannyh/zbmath
– Архив журналов РАН https://lib.tusur.ru/ru/resursy/bazy-dannyh/arhiv-zhurnalov-ran
– Университетская информационная система РОССИЯ – https://uisrussia.msu.ru/

14. Материально-техническое обеспечение

Аудитории для проведения занятий лекционного типа.

Аудитории для проведения занятий семинарского типа, индивидуальных и групповых консультаций, текущего контроля и промежуточной аттестации.

Помещения для самостоятельной работы, оснащенные компьютерной техникой и доступом к сети Интернет, в электронную информационно-образовательную среду и к информационным справочным системам.

Лаборатории 2-го корп., оборудованные для проведения занятий в Moodl: 324, 316 и 319.

Аудитории для проведения занятий лекционного и семинарского типа индивидуальных и групповых консультаций, текущего контроля и промежуточной аттестации в смешенном формате («Актру»). Это аудитории 2-го корп.: 428, 121, 124, 302, 411, 423.

15. Информация о разработчиках

Чехлов Андрей Ростиславович, д.ф.-м.н., профессор каф. алгебры ТГУ.