

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

Механико-математический факультет

УТВЕРЖДАЮ:

Декан



Л. В. Гензе

« 30 » 06 20 22 г.

Рабочая программа дисциплины

**Теория чисел**

по направлению подготовки

**01.03.01 Математика, 02.03.01 Математика и компьютерные науки**

Направленность (профиль) подготовки :

**Основы научно-исследовательской деятельности в области математики,  
Основы научно-исследовательской деятельности в области математики и  
компьютерных наук**

Форма обучения

**Очная**

Квалификация

**Бакалавр**

Год приема

2022, 2023

Код дисциплины в учебном плане: Б1.В.2.07

СОГЛАСОВАНО:

Руководитель ОП



Л. В. Гензе

Председатель УМК



Е. А. Тарасов

Томск – 2022

## **1. Цель и планируемые результаты освоения дисциплины**

Целью освоения дисциплины является формирование следующих компетенций:

ОПК-1 Способен применять фундаментальные знания в области математического анализа, комплексного и функционального анализа, алгебры, аналитической геометрии, дифференциальной геометрии и топологии, дифференциальных уравнений, дискретной математики и математической логики, теории вероятностей, математической статистики и случайных процессов, численных методов, теоретической механики как для использования в профессиональной деятельности, так и для консультирования.

Результатами освоения дисциплины являются следующие индикаторы достижения компетенций:

ИОПК 1.1 Демонстрирует навыки работы с профессиональной литературой по основным естественнонаучным и математическим дисциплинам

ИОПК 1.2 Демонстрирует навыки выполнения стандартных действий, решения типовых задач с учетом основных понятий и общих закономерностей, формулируемых в рамках базовых математических и естественнонаучных дисциплин

ИОПК 1.3 Владеет фундаментальными знаниями, полученными в области математических и (или) естественных наук

## **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.

## **3. Место дисциплины в структуре образовательной программы**

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

Дисциплина относится к обязательной части образовательной программы.

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

Шестой семестр, зачет

## **5. Входные требования для освоения дисциплины**

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

## **6. Язык реализации**

Русский

## **7. Объем дисциплины**

Общая трудоемкость дисциплины составляет 3 з.е., 108 часов, из которых:

-лекции: 32 ч.

-практические занятия: 32 ч.

в том числе практическая подготовка: 0 ч.

Объем самостоятельной работы студента определен учебным планом.

## 8. Содержание дисциплины, структурированное по темам

### Тема 1. Делимость и простые числа.

Теорема о делении с остатком. НОД чисел. Алгоритм Евклида. Простые числа. Основная теорема арифметики.

### Тема 2. Арифметические функции.

Мультипликативные функции и их примеры.

### Тема 3. Цепные дроби.

### Тема 4. Сравнения 1-й степени.

### Тема 5. Сравнения $n$ -степени.

### Тема 6. Сравнения 2-степени.

### Тема 7. Первообразные корни и индексы.

## 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

Зачет в шестом семестре проводится в письменной форме по билетам. Билет содержит теоретический вопрос и две задачи. Продолжительность зачета 1,5 часа.

Примерный перечень теоретических вопросов

1. Вопрос 1. Мультипликативность функции  $\tau(n)$ . Доказать, что если  $n = p^\alpha \dots q^\gamma$  – каноническое разложение числа  $n$ , то  $\tau(n) = (\alpha + 1) \dots (\gamma + 1)$ .

2. Вопрос 2. Докажите теорему о разрешимости в  $\mathbb{Z}$  уравнения  $ax + by = c$ , где  $a, b, c$  – целые числа и  $ab \neq 0$

3. Вопрос 3. Докажите, что если  $a$  – квадратичный вычет по модулю  $p$ , то  $a^{(p-1)/2} \equiv 1 \pmod{p}$ .

Вопрос 4. Теория чисел и криптосистема RSA.

Примеры задач:

1. Найдите двузначное число, сравнимое с 2 по модулю 3 и 7, и с -2 по модулю 11.

2. Решите сравнение  $2x - 3y \equiv 4 \pmod{5}$ .

3. Разложите число  $539/103$  в цепную дробь.

4. Исследовать, какие из чисел между 2320 и 2350 являются простыми.

Вид оцениваемой работы:	Удельный вес указанного вида работы в итоговой оценке (в процентах)	В течение семестра/в конце семестра	Критерии оценивания указанного вида работы
Инд. задание в системе Moodle.	20%	В течение семестра	По 100 бальной системе.
Тесты в системе Moodle.	30%	В течение семестра	Максимальное использование возможностей программы
Зачет	50%	В конце семестра	Студент допускается до зачета только при наличии выполненных индивидуального задания и теста. 1) Полный ответ, изложенный кратко и ясно – «зачет». 2) Ответ неполный (но >

			50%), пояснения логически непротиворечивы – «зачет». 3) Ответ неполный (< 50%), отсутствие логики в пояснениях – «незачет». 4) Ответ по сути отсутствует – «незачет».
--	--	--	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------

## 11. Учебно-методическое обеспечение

а) Электронный учебный курс по дисциплине в электронном университете «Moodle» - <https://moodle.tsu.ru/course/view.php?id=12937>

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. Делимость и простые числа. Теорема о делении с остатком. НОД чисел. Алгоритм Евклида. Простые числа. Основная теорема арифметики.	4	4			4	
2. Арифметические функции. Мультипликативные функции и их примеры.	5	5			4	
3. Цепные дроби.	4	4			4	
4. Сравнения 1-й степени	5	5			5	
5. Индивидуальное задание					6	Задание в системе Moodle.
6. Сравнения n-степени.	4	4			4	
7. Сравнения 2-степени	4	4			6	
8. Первообразные корни и индексы.	6	6			5,55	
9. Тесты					2	Тесты в системе Moodle.
Всего 108	32	32		3,45	40,55	

Аттестация во время контрольной точки №1 ставится в случае выполнения 1-й контрольной работы и активной работы на лекциях и практических занятиях.

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 нижеприведимом 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. Кузьмина А. С., Мальцев Ю. Н. Теория чисел. Барнаул, 2011. 240 с.
2. Бухштаб А. А. Теория чисел. Лань. 2015. 384 с.
3. Виноградов, И.М. Основы теории чисел. 2003. 176 с.

б) дополнительная литература:

1. Деза Е. И., Котова Л. В. Сборник задач по теории чисел. М.: Либроком/URSS, 2012. 224 с.
2. Манин Ю. И., Панчишкин А.А. Введение в современную теорию чисел. М.: МЦНМО, 2013. 552 с.
3. Сушкевич А.К. Теория чисел. М.: Вузовская книга, 2016. 240 с.
4. Арнольд И.В. Теория чисел. М.: Ленанд, 2019. – 288 с.
5. Борович З.И., Шафаревич И.Р. Теория чисел. М.: Ленанд, 2019. – 504 с.
6. Куликов Л. Я., Москаленко А. И., Фомин А. А. Сборник задач по алгебре и теории чисел. М.: Просвещение, 1993. 288 с.

в) ресурсы сети Интернет.

Открытые онлайн-курсы по теории чисел:

1. <https://www.youtube.com/playlist?list=PL2ar10WmyGU5A6qkfwbujIMJYXR6S5PiP>
2. <https://openedu.ru/course/eltech/DisMath/>
3. [https://ru.wikipedia.org/wiki/Теория\\_чисел](https://ru.wikipedia.org/wiki/Теория_чисел)
4. 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:

- [www.elibrary.ru](http://www.elibrary.ru)
- Russian Science Citation Index (RSCI) – <https://clarivate.ru/products/web-of-science-rsci>
- [Scopus](https://lib.tusur.ru/ru/resursy/bazy-dannyh/scopus) <https://lib.tusur.ru/ru/resursy/bazy-dannyh/scopus>
- [zbMATH](https://lib.tusur.ru/ru/resursy/bazy-dannyh/zbmath) <https://lib.tusur.ru/ru/resursy/bazy-dannyh/zbmath>
- [Архив журналов РАН](https://lib.tusur.ru/ru/resursy/bazy-dannyh/arhiv-zhurnalov-ran) <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 корпуса ТГУ, оборудованные для проведения занятий в Moodle: 314, 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.