

Министерство науки и высшего образования РФ  
Федеральное государственное автономное образовательное учреждение  
высшего образования  
«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»  
**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)**

Б1.В.03 Теория чисел

---

наименование дисциплины (модуля) в соответствии с учебным планом

Направление подготовки / специальность

01.03.04 Прикладная математика

---

Направленность (профиль)

01.03.04 Прикладная математика

---

Форма обучения

очная

---

Год набора

2020

---

Красноярск 2022

## РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Программу составили \_\_\_\_\_

Осипов Н.Н.

\_\_\_\_\_  
должность, инициалы, фамилия

## 1 Цели и задачи изучения дисциплины

### 1.1 Цель преподавания дисциплины

Знание основ теории чисел полезно и зачастую даже необходимо в работе будущего специалиста в области прикладной математики. Теоретико-числовые методы наряду с классическими методами математического и функционального анализа применяются в различных разделах современной вычислительной математики. Хорошо известны приложения теории чисел (в том числе и элементарной) к криптографии.

Целью преподавания дисциплины «Теория чисел» является изложение основ элементарной теории чисел (делимость целых чисел, алгоритм Евклида, сравнения по модулю, линейные диофантовы уравнения, первообразные корни), а также некоторых результатов аналитической теории чисел (классические оценки Чебышёва для функции распределения простых чисел), допускающих обоснование элементарными средствами (без привлечения методов теории функций комплексного переменного).

### 1.2 Задачи изучения дисциплины

В результате изучения дисциплины «Теория чисел» студенты должны знать основные понятия и факты, относящиеся к элементарной теории чисел; уметь

решать задачи элементарной теории чисел; владеть навыками в употреблении модулярной арифметики, стандартными эффективными вычислительными алгоритмами в элементарной теории чисел.

### 1.3 Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы

Код и наименование индикатора достижения компетенции	Запланированные результаты обучения по дисциплине
<b>ПК-1: Способен к постижению основ математических моделей реального объекта или процесса, готов применять моделирование для построения объектов и процессов, определения или предсказания их свойств.</b>	
ПК-1.1: Знать основы применения математических моделей при исследовании процессов и систем.	отношение делимости, деление с остатком; НОД и НОК целых чисел, алгоритм Евклида, свойства взаимно простых чисел; простые и составные числа, каноническое разложение, основная теорема арифметики; основные теоретико-числовые функции, их свойства и способы вычисления; оценки Чебышёва для функции $\pi(x)$ ; асимптотический закон распределения простых чисел решать задачи элементарной теории чисел основными понятиями и фактами, относящимися к элементарной теории чисел

ПК-1.2: Уметь использовать современный аппарат математического моделирования при решении	определение числовых сравнений и их свойства; сравнения с неизвестным и методы их решения; алгоритм решения сравнений 1-й степени; алгоритм решения линейных диофантовых уравнений с двумя
прикладных научных и производственных задач	неизвестными; решать задачи на делимость и простейшие типы диофантовых уравнений навыками в употреблении модулярной арифметики
ПК-1.3: Владеть методами проверки на адекватность и проведения анализа результатов моделирования.	система шифрования RSA; бинарный алгоритм возведения в степень по модулю, понятие псевдопростого числа, строго псевдопростого числа, способ генерации больших простых чисел применять технику сравнений по модулю (или метод остатков), стандартными эффективными вычислительными алгоритмами в элементарной теории чисел (на базе алгоритма Евклида и алгоритма быстрого возведения в степень по модулю).
<b>ПК-3: Способен применять математический аппарат для решения поставленных задач.</b>	
ПК-3.1: Знать основы применения математического аппарата для решения поставленных задач.	основные методы элементарной теории чисел и основные результаты аналитической теории чисел применять методы модулярной арифметики в прикладных задачах (обработка изображений, криптография, алгебраическая теория кодирования) основными вычислительными приемами элементарной теории чисел
ПК-3.2: Уметь самостоятельно разрабатывать математические модели, на основе содержательного и физического описания процессов и объектов.	первообразные корни по модулю, теорема о существовании первообразного корня по простому модулю применять первообразные корни по модулю, теорема о существовании первообразного корня по простому модулю основными вычислительными алгоритмами элементарной теории чисел
ПК-3.3: Владеть основными понятиями и результатами основополагающих математических дисциплин;	классы вычетов по модулю, группа обратимых (взаимно простых с модулем) классов вычетов; порядок обратимого класса вычетов; применять методы алгебры многочленов и математического анализа при решении указанных задач навыками в употреблении абстрактных алгебраических структур при решении теоретико-числовых задач

#### 1.4 Особенности реализации дисциплины

Язык реализации дисциплины: Русский.

Дисциплина (модуль) реализуется с применением ЭО и ДОТ

URL-адрес и название электронного обучающего курса: <https://e.sfu->

kras.ru/course/view.php?id=978.

## 2. Объем дисциплины (модуля)

Вид учебной работы	Всего, зачетных единиц (акад.час)	е
		1
<b>Контактная работа с преподавателем:</b>	<b>2 (72)</b>	
занятия лекционного типа	1 (36)	
практические занятия	1 (36)	
<b>Самостоятельная работа обучающихся:</b>	<b>1 (36)</b>	
курсовое проектирование (КП)	Нет	
курсовая работа (КР)	Нет	
<b>Промежуточная аттестация (Экзамен)</b>	<b>1 (36)</b>	

### 3 Содержание дисциплины (модуля)

#### 3.1 Разделы дисциплины и виды занятий (тематический план занятий)

		Контактная работа, ак. час.							
№ п/п	Модули, темы (разделы) дисциплины	Занятия лекционного типа		Занятия семинарского типа				Самостоятельная работа, ак. час.	
				Семинары и/или Практические занятия		Лабораторные работы и/или Практикумы			
		Всего	В том числе в ЭИОС	Всего	В том числе в ЭИОС	Всего	В том числе в ЭИОС	Всего	В том числе в ЭИОС
<b>1. Теория делимости</b>									
	1. Делимость целых чисел. Наибольший общий делитель	2							
	2. Взаимно простые числа. Наименьшее общее кратное. Китайская теорема об остатках	2							
	3. Простые и составные числа	2							
	4. Основная теорема арифметики и её следствия	2							
	5. Мультипликативные функции	2							
	6. Целая и дробная часть числа	2							
	7. Оценки Чебышёва	2							
	8. Асимптотический закон распределения простых чисел	2							

9. Решение задач на делимость целых чисел. Вычисление наибольшего общего делителя и его линейной формы при помощи алгоритма Евклида. Вычисление наибольшего общего делителя нескольких чисел.			2					
10. Связь между наибольшим общим делителем и наименьшим общим кратным двух чисел. Вычисление наименьшего общего кратного нескольких чисел. Свойства взаимно простых чисел.			2					
11. Различные приложения китайской теоремы об остатках. Определение простого (или составного) характера чисел. Доказательство методом Евклида бесконечности простых чисел в некоторых арифметических прогрессиях. Практическая реализация решета Эратосфена.			2					
12. Основная теорема арифметики. Вычисление наибольшего общего делителя и наименьшего общего кратного при помощи канонических разложений.			2					
13. Приложение основной теоремы арифметики к решению задач на делимость и некоторых диофантовых уравнений			2					
14. Теория делимости							16	
<b>2. Теория сравнений и кольца классов вычетов</b>								
1. Определение и свойства сравнений	2							
2. Классы вычетов. Теоремы Ферма и Эйлера	2							
3. Сравнения с неизвестными	2							
4. Сравнения первой степени	2							
5. Кольцо $Z_m$ классов вычетов по модулю $m$	2							

6. Группа обратимых элементов кольца $Z_m$	2							
7. Поле $Z_p$ классов вычетов по простому модулю $p$	2							
8. Порядок класса вычетов. Первообразные корни	2							
9. Доказательство тождеств и решение уравнений и неравенств, содержащих знаки целой и дробной части. Вычисление значений различных мультипликативных функций: числа делителей, суммы делителей, функции Эйлера, функции Мёбиуса.			2					
10. Приложения формулы Лежандра. Применение оценок Чебышёва и постулата Бертрана в решении различных теоретико-числовых задач.			2					
11. Контрольная работа № 1 по теме «Теория делимости»			2					
12. Применение техники сравнений (переход от чисел к классам вычетов по некоторому модулю). Полная и приведенная системы вычетов, их свойства.			2					
13. Приложение малой теоремы Ферма и теоремы Эйлера к решению задач. Функция Кармайкла.			2					
14. Переборный алгоритм решения сравнений с одним и несколькими неизвестными. Решение сравнений (с одним неизвестным) по простому модулю.			2					
15. Алгоритм Евклида для решения сравнений 1-й степени и их систем. Решение неопределенных (диофантовых) уравнений 1-й степени с двумя неизвестными.			2					



16. Выполнение арифметических действий в кольце классов вычетов $Z_m$ : сложение, вычитание, умножение. Вычисления в группе обратимых элементов кольца $Z_m$ : отыскание обратного класса вычетов, возведение класса вычетов в степень. Деление в кольце $Z_m$ на обратимый класс вычетов $Z_m$			2					
17. Модулярная арифметика (арифметика поля $Z_p$ ) и ее приложения к решению различных теоретико-числовых задач. Многочлены над полем $Z_p$ . Теорема Вильсона и ее следствия.			2					
18. Вычисление порядка числа по модулю. Отыскание первообразных корней по простому модулю и по модулю степени простого числа.			2					
19. Контрольная работа №2 по теме «Теория сравнений и кольца классов вычетов»			2					
20. Теория сравнений и кольца классов вычетов							16	
<b>3. Приложение к криптографии</b>								
1. Система шифрования RSA	2							
2. Псевдопростые числа	2							
3. Система шифрования RSA. Бинарный алгоритм возведения числа в большую степень по модулю. Критерии и достаточные условия простоты чисел. Генерация больших простых чисел.			2					
4. Различные тесты псевдопростоты и их практическая реализация. Вероятностный тест строгой псевдопростоты Миллера-Рабина, как эффективный способ отличить составное число от простого.			2					
5. Приложение к криптографии							4	
6.								

Bcero	36		36				36	
-------	----	--	----	--	--	--	----	--

## **4 Учебно-методическое обеспечение дисциплины**

### **4.1 Печатные и электронные издания:**

1. Виноградов И. М. Основы теории чисел: учебное пособие(Москва: Лань).
2. Галочкин А. И., Нестеренко Ю. В., Шидловский А. Б., Шидловский А. Б. Введение в теорию чисел: учебное пособие для вузов по специальности "Математика"(Москва: МГУ им. М. В. Ломоносова).
3. Кириллова С. В. Теоретико-числовые методы в криптографии. Криптографическая система RSA: учеб-метод. пособие для студентов спец. 090301.65 (090102.65) «Компьютерная безопасность» и направления 090900.62 «Информационная безопасность».(Красноярск: СФУ).
4. Нестеренко Ю.В., Амаатов М.А. Теория чисел: учебник для вузов.; допущено УМО по классическому университетскому образованию(М.: Академия).
5. Гашков С. Б., Чубариков В. Н. Арифметика. Алгоритмы. Сложность вычислений: учебное пособие для вузов по направлениям и специальностям физико-математического профиля(Москва: МГУ им. М. В. Ломоносова).
6. Борович З. И., Шафаревич И. Р. Теория чисел(Москва: Наука, Гл. ред. физ.-мат. лит.).
7. Осипов Н. Н., Медведева М. И. Теория чисел: учебное пособие [для студентов специальности 01.03.04 «Прикладная математика»] (Красноярск: СФУ).

### **4.2 Лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства (программное обеспечение, на которое университет имеет лицензию, а также свободно распространяемое программное обеспечение):**

1. Методика проведения занятий допускает использование технических средств (проекторы, интерактивные доски), обеспеченных соответствующим программным обеспечением, предлагается применение вычислительной техники и стандартных пакетов прикладных программ.

### **4.3 Интернет-ресурсы, включая профессиональные базы данных и информационные справочные системы:**

1. Наличие электронно-библиотечной системы (электронной библиотеки) и электронной информационно-образовательной среды СФУ, которые обеспечивают возможность индивидуального доступа для каждого обучающегося из любой точки, в которой имеется доступ к сети Интернет, как на территории СФУ, так и вне университета.

## **5 Фонд оценочных средств**

Оценочные средства находятся в приложении к рабочим программам дисциплин.

## **6 Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине (модулю)**

Методика проведения занятий допускает как использование технических средств (проекторы, интерактивные доски), так и классические аудиторные занятия, обеспечиваемые стандартными материально-техническими средствами