

**Федеральное государственное автономное образовательное  
учреждение высшего образования  
«Московский физико-технический институт  
(национальный исследовательский университет)»**

**УТВЕРЖДЕНО**

**Директор физтех-школы  
прикладной математики и  
информатики**

**А.М. Райгородский**

	<b>Рабочая программа дисциплины (модуля)</b>
<b>по дисциплине:</b>	Теория чисел и алгебро-геометрическое кодирование
<b>по направлению:</b>	Информатика и вычислительная техника
<b>профиль подготовки:</b>	Прикладная математика и информатика Физтех-школа Прикладной Математики и Информатики кафедра дискретной математики
<b>курс:</b>	2
<b>квалификация:</b>	магистр

Семестр, формы промежуточной аттестации: 3 (осенний) - Дифференцированный зачет

Аудиторных часов: 60 всего, в том числе:

лекции: 0 час.

семинары: 60 час.

лабораторные занятия: 0 час.

Самостоятельная работа: 30 час.

Всего часов: 90, всего зач. ед.: 2

Количество контрольных работ, заданий: 2

Программу составил: А.Б. Дайняк, канд. физ.-мат. наук, доцент

Программа обсуждена на заседании кафедры дискретной математики 05.03.2020

## Аннотация

В курсе будет изложен целый ряд как классических, так и современных результатов теории чисел, связанных с диофантовыми приближениями и трансцендентными числами, распределением простых чисел и нулями дзета-функции Римана, анализом Фурье на конечных абелевых группах. Кроме того, курс предусматривает разбор и самостоятельное решение наиболее характерных задач по перечисленным разделам. Для освоения курса желательно знание основ алгебры и теории функций комплексного переменного, однако большая часть необходимых сведений будет дана слушателям по ходу изложения.

### 1. Цели и задачи

#### Цель дисциплины

освоение основных современных алгебраических методов в теории чисел.

#### Задачи дисциплины

- освоение студентами базовых знаний (понятий, концепций, методов и моделей) в теории алгебраических методов в теории чисел;
- приобретение теоретических знаний и практических умений и навыков в теории алгебраических методов в теории чисел;
- оказание консультаций и помощи студентам в проведении собственных теоретических ис-следований в теории алгебраических методов в теории чисел.

### 2. Перечень формируемых компетенций

Освоение дисциплины направлено на формирование следующих компетенций:

Код и наименование компетенции	Индикаторы достижения компетенции
ОПК-1 Владеет системой фундаментальных научных знаний в области информатики и вычислительной техники	ОПК-1.1 Знает и способен использовать в профессиональной деятельности фундаментальные научные знания и новые научные принципы и методы исследований в области информатики и вычислительной техники
ОПК-2 Имеет представление об актуальных проблемах науки и техники в области информатики и вычислительной техники, способен на научном языке формулировать профессиональные задачи	ОПК-2.1 Имеет представление о современном состоянии исследований в рамках тематической области своей профессиональной деятельности
ОПК-4 Способен успешно реализовывать решение поставленной задачи, провести анализ результата и представить выводы, применяя знания и навыки в области математики, естественных наук и информационно-коммуникационных технологий	ОПК-4.1 Способен применять знания и навыки по использованию информационно-коммуникационных технологий для поиска и изучения научной литературы, применения прикладных программных продуктов

### 3. Перечень планируемых результатов обучения по дисциплине (модулю)

В результате освоения дисциплины обучающиеся должны

знать:

- фундаментальные понятия, законы, теории алгебраических методов в теории чисел;
- современные проблемы соответствующих разделов теории алгебраических методов в теории чисел;
- понятия, аксиомы, методы доказательств и доказательства основных теорем в разделах, входящих в базовую часть цикла теории алгебраических методов в теории чисел;
- основные свойства соответствующих математических объектов;
- аналитические и численные подходы и методы для решения типовых прикладных задач теории алгебраических методов в теории чисел.

уметь:

понять поставленную задачу;  
 использовать свои знания для решения фундаментальных и прикладных задач;  
 оценивать корректность постановок задач;  
 строго доказывать или опровергать утверждение;  
 самостоятельно находить алгоритмы решения задач, в том числе и нестандартных, и проводить их анализ;  
 самостоятельно видеть следствия полученных результатов;  
 точно представить математические знания в устной и письменной форме.

владеть:

навыками освоения большого объема информации и решения задач ( в том числе, сложных);  
 навыками самостоятельной работы и освоения новых дисциплин;  
 культурой постановки, анализа и решения математических и прикладных задач, требующих для своего решения использования математических подходов и методов;  
 предметным языком топологии и навыками грамотного описания решения задач и представления полученных результатов.

#### 4. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

##### 4.1. Разделы дисциплины (модуля) и трудоемкости по видам учебных занятий

№	Тема (раздел) дисциплины	Трудоемкость по видам учебных занятий, включая самостоятельную работу, час.			
		Лекции	Семинары	Лаборат. работы	Самост. работа
1	Теорема о рекуррентном неравенстве		14		6
2	Параллельное вычисление префиксов «произведения» $n$ элементов для ассоциативной операции		14		6
3	Теорема Липтона—ДеМилло—Шварца—Зиппеля		12		6
4	Понятие о задаче ранжирования в поисковых системах		10		6
5	Понятие кода, исправляющего ошибки. Границы Хемминга и Плоткина		10		6
Итого часов			60		30
Подготовка к экзамену		0 час.			
Общая трудоёмкость		90 час., 2 зач.ед.			

##### 4.2. Содержание дисциплины (модуля), структурированное по темам (разделам)

Семестр: 3 (Осенний)

###### 1. Теорема о рекуррентном неравенстве

Решение дискретной задачи как вычисление набора булевых функций. Схемы из функциональных элементов (алгоритм  $\rightarrow$  последовательность схем). Меры сложности схем: размер и глубина, связь глубины и времени вычисления ответа схемой. Базисы  $B_0$  и  $B_2$ . Эквивалентность базисов с точки зрения порядка роста размера и глубины схем. Оценки глубины схем, построенных по формулам, через их размер. Классы NC и AC.

## 2. Параллельное вычисление префиксов «произведения» n элементов для ассоциативной операции

Сложность «самых сложных функций» от n аргументов. Верхняя оценка числа схем с данным числом входов и данной сложностью. Нижняя асимптотическая оценка  $2^n/n$  (мощностной метод — если сложность маленькая, то схем не хватит). Эффект Шеннона: почти все функции сложны. Замечание о гигантской разнице между известными оценками для почти всех функций и нижними оценками для конкретных функций. Асимптотически оптимальная схема для дешифратора (индукция → трюк meet-in-the-middle).

## 3. Теорема Липтона—ДеМилло—Шварца—Зиппеля

Вычисление определителя и обращение матриц в классе NC: алгоритм Чанского.

## 4. Понятие о задаче ранжирования в поисковых системах

Аналогичное применение подхода «разделяй и властвуй» в умножении матриц: алгоритм Штрассена.

## 5. Понятие кода, исправляющего ошибки. Границы Хемминга и Плоткина

Применение линейного программирования в задаче о покрытии. Простое округление в задаче о взвешенном вершинном покрытии графа. Вероятностное округление в задаче о покрытии множеств. Основанный на двойственности комбинаторный алгоритм для задачи о взвешенном вершинном покрытии.

## 5. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)

Стандартная учебная аудитория.

## 6. Перечень рекомендуемой литературы

### Основная литература

1. Языки и исчисления [Текст] : лекции по мат. логике и теории алгоритмов / Н. К. Верещагин, А. Шень .— 3-е изд., доп. — М. : МЦНМО, 2008 .— 288 с.
2. Алгоритмы [Текст] : [учеб. пособие для вузов] / С. Дасгупта, Х. Пападимитриу, У. Вазириани ; пер. с англ. А. А. Куликова ; под ред. А. Шеня .— М. : МЦНМО, 2014 .— 320 с.
3. Введение в теорию автоматов, языков и вычислений [Текст] /Д. Хопкрофт, Р. Мотвани, Д. Ульман ; пер. с англ. О. И. Васылык [и др.], [учеб. пособие для вузов]. -М, Вильямс, 2018
4. Заметки по теории кодирования [Текст] / А. Е. Ромащенко, А. Ю. Румянцев, А. Шен .— [Учебное изд.] .— М : МЦНМО, 2011 .— 80 с.

### Дополнительная литература

1. Лекции по алгебраическому кодированию [Текст] : учеб. пособие для вузов / Э. М. Габидулин ; М-во образования и науки РФ, Моск. физ.-техн. ин-т (гос. ун-т) .— М. : МФТИ, 2015 .— 107 с.

## 7. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины (модуля)

<http://dm.fizteh.ru/>

## 8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень необходимого программного обеспечения и информационных справочных систем (при необходимости)

На лекционных занятиях используются мультимедийные технологии, включая демонстрацию презентаций.

В процессе самостоятельной работы обучающихся возможно использование таких программных средств, как Mathcad, MATLAB, Maple и др.

## **9. Методические указания для обучающихся по освоению дисциплины (модуля)**

1. Рекомендуется успешно сдавать контрольные работы, так как это упрощает итоговую аттестацию по предмету.
2. Для подготовки к итоговой аттестации по предмету лучше всего пользоваться материалами лекций.

**ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)**

**по направлению:** Информатика и вычислительная техника  
**профиль подготовки:** Прикладная математика и информатика  
Физтех-школа Прикладной Математики и Информатики  
кафедра дискретной математики  
**курс:** 2  
**квалификация:** магистр

Семестр, формы промежуточной аттестации: 3 (осенний) - Дифференцированный зачет

**Разработчик:** А.Б. Дайняк, канд. физ.-мат. наук, доцент

## 1. Компетенции, формируемые в процессе изучения дисциплины

Код и наименование компетенции	Индикаторы достижения компетенции
ОПК-1 Владеет системой фундаментальных научных знаний в области информатики и вычислительной техники	ОПК-1.1 Знает и способен использовать в профессиональной деятельности фундаментальные научные знания и новые научные принципы и методы исследований в области информатики и вычислительной техники
ОПК-2 Имеет представление об актуальных проблемах науки и техники в области информатики и вычислительной техники, способен на научном языке формулировать профессиональные задачи	ОПК-2.1 Имеет представление о современном состоянии исследований в рамках тематической области своей профессиональной деятельности
ОПК-4 Способен успешно реализовывать решение поставленной задачи, провести анализ результата и представить выводы, применяя знания и навыки в области математики, естественных наук и информационно-коммуникационных технологий	ОПК-4.1 Способен применять знания и навыки по использованию информационно-коммуникационных технологий для поиска и изучения научной литературы, применения прикладных программных продуктов

## 2. Показатели оценивания компетенций

В результате изучения дисциплины «Теория чисел и алгебро-геометрическое кодирование» обучающийся должен:

### знать:

фундаментальные понятия, законы, теории алгебраических методов в теории чисел;  
современные проблемы соответствующих разделов теории алгебраических методов в теории чисел;

понятия, аксиомы, методы доказательств и доказательства основных теорем в разделах, входящих в базовую часть цикла теории алгебраических методов в теории чисел;

основные свойства соответствующих математических объектов;

аналитические и численные подходы и методы для решения типовых прикладных задач теории алгебраических методов в теории чисел.

### уметь:

понять поставленную задачу;

использовать свои знания для решения фундаментальных и прикладных задач;

оценивать корректность постановок задач;

строго доказывать или опровергать утверждение;

самостоятельно находить алгоритмы решения задач, в том числе и нестандартных, и проводить их анализ;

самостоятельно видеть следствия полученных результатов;

точно представить математические знания в топологии в устной и письменной форме.

### владеть:

навыками освоения большого объема информации и решения задач ( в том числе, сложных);

навыками самостоятельной работы и освоения новых дисциплин;

культурой постановки, анализа и решения математических и прикладных задач, требующих для своего решения использования математических подходов и методов;

предметным языком топологии и навыками грамотного описания решения задач и представления полученных результатов.

## 3. Перечень типовых (примерных) вопросов, заданий, тем для подготовки к текущему контролю

1. Решить в целых числах уравнение  $x^2 + 1 = 3y$ .

2. Найти две последние цифры числа  $2^{100}$ .

3. Вывести теорему Эйлера из теоремы Ферма

4. Найти количество вещественных характеров по модулю 12.

5. Найти все первообразные корни по модулю 25.
6. Доказать формулу обращения для преобразования Фурье на конечной абелевой группе
7. Доказать равенство Парсеваля для преобразования Фурье на конечной абелевой группе

#### 4. Перечень типовых (примерных) вопросов и тем для проведения промежуточной аттестации обучающихся

Теорема о рекуррентном неравенстве. [Cormen, §4.5]

Решение дискретной задачи как вычисление набора булевых функций. Схемы из функциональных элементов (алгоритм  $\rightarrow$  последовательность схем). Базисы  $B_0$  и  $B_2$ . Эквивалентность базисов с точки зрения порядка роста размера и глубины схем. Меры сложности схем: размер и глубина, связь глубины и времени вычисления ответа схемой. Оценки глубины схем, построенных по формулам, через их размер. Классы NC и AC. [ВерещагинШень, §1.3, Теоремы 7 и 16]

Сложность «самых сложных функций» от  $n$  аргументов. Верхняя оценка числа схем с данным числом входов и данной сложностью. Нижняя асимптотическая оценка  $2n/n$  (мощностной метод — если сложность маленькая, то схем не хватит). Эффект Шеннона: почти все функции сложны. Замечание о гигантской разнице между известными оценками для почти всех функций и нижними оценками для конкретных функций. Асимптотически оптимальная схема для дешифратора (индукция  $\rightarrow$  трюк meet-in-the-middle). Оптимальная схема для универсального многополюсника (произвольная схема  $\rightarrow$  топологическая сортировка  $\rightarrow$  устранение дублирования). Формула разложения булевой функции по нескольким переменным. Верхняя оценка сложности самой сложной функции  $10 \times 2n/n$ . [Wegener, §4.1, §4.2]

Параллельное вычисление префиксов «произведения»  $n$  элементов для ассоциативной операции. [Kozen, §28.3] Применения: построение схем логарифмической глубины для сравнения и сложения чисел. Вычитание (дополнительный код), умножение (3-2 трюк), деление (метод Ньютона). [Kozen, §30] (Если нет возможности читать Kozen, можно обратиться к [ВерещагинШень, §1.3].)

Вычисление определителя и обращение матриц в классе NC: алгоритм Чанского. [Kozen, §31]

Схема субквадратичного размера для умножения чисел: алгоритм Карацубы—Офмана [ВерещагинШень, §1.3, Теорема 13]. Аналогичное применение подхода «разделяй и властвуй» в умножении матриц: алгоритм Штрассена. [АхоХопкрофтУльман, §6.2]

Теорема Липтона—ДеМилло—Шварца—Зиппеля (лемма Шварца—Зиппеля). [Kozen, §40] Лемма об изолировании (теорема Малмалы—Вазирани—Вазирани). [Jukna, §11.3]

Классы RP, co-RP и ZPP. Равенство  $RP \cap co-RP = ZPP$ . [Cai, §5.4] Применение леммы Шварца—Зиппеля в задаче о существовании совершенного паросочетания (вычисление определителя матрицы смежности двудольного графа). [Kozen, §40.1]

Вероятностный параллельный алгоритм нахождения совершенного паросочетания в двудольном графе [MotwaniRaghavan, §12.4.2]

Теорема Вигдерсона о моделировании контактных схем схемами чётности. [Jukna 1st edition, Theorem 12.6]

Дискретное преобразование Фурье. Связь с задачей умножения многочленов. Замечание о применении в обработке сигналов. Алгоритм быстрого преобразования Фурье. [Дасгупта, §2.6] Алгоритм Шёнхаге—Штрассена. [АхоХопкрофтУльман, гл. 7]

Понятие о задаче ранжирования в поисковых системах. Случайное блуждание по веб-графу: PageRank. Система линейных уравнений для его вычисления. Ещё одно применение систем линейных уравнений: визуализация графов с помощью теоремы Татта о «пружинной укладке».

Применение линейного программирования в задаче о покрытии. Простое округление в задаче о взвешенном вершинном покрытии графа. Вероятностное округление в задаче о покрытии множеств. Основанный на двойственности комбинаторный алгоритм для задачи о взвешенном вершинном покрытии. [Trevisan, §7]

Понятие кода, исправляющего ошибки. Границы Хемминга и Плоткина. Матрицы Адамара (+ набросок доказательства теоремы Адамара). Использование матриц Адамара для построения кодов, на которых достигается граница Плоткина. Коды Хемминга (на которых достигается граница Хемминга). [РомащенкоРумянцевШень] [методичка]

Применение теории групп в информатике. Теорема Баррингтона о построении BDD константной ширины по булевой формуле с полиномиальным ростом сложности. [Wikipedia]



## Критерии оценивания

- оценка «отлично (10)» выставляется студенту, показавшему всесторонние, систематизированные, глубокие знания учебной программы дисциплины и умение уверенно применять их на практике при решении конкретных задач, свободное и правильное обоснование принятых решений
- оценка «отлично (9)» выставляется студенту, показавшему всесторонние, систематизированные, глубокие знания учебной программы дисциплины и умение применять их на практике при решении конкретных задач, свободное и правильное обоснование принятых решений
- оценка «отлично (8)» выставляется студенту, показавшему всесторонние систематизированные, глубокие знания учебной программы дисциплины и умение применять их на практике при решении конкретных задач, и правильное обоснование принятых решений
- оценка «хорошо (7)» выставляется студенту, если он твердо знает материал, грамотно и по существу излагает его, умеет применять полученные знания на практике, но допускает в ответе или в решении задач некоторые неточности;
- оценка «хорошо (6)» выставляется студенту, если он знает материал, грамотно и по существу излагает его, умеет применять полученные знания на практике, но допускает в ответе или в решении задач некоторые неточности;
- оценка «хорошо (5)» выставляется студенту, если он знает материал, и по существу излагает его, умеет применять полученные знания на практике, но допускает в ответе или в решении задач некоторые неточности;
- оценка «удовлетворительно (4)» выставляется студенту, показавшему фрагментарный, разрозненный характер знаний, недостаточно правильные формулировки базовых понятий, нарушения логической последовательности в изложении программного материала, но при этом он владеет основными разделами учебной программы, необходимыми для дальнейшего обучения и может применять полученные знания по образцу в стандартной ситуации;
- оценка «удовлетворительно (3)» выставляется студенту, показавшему фрагментарный, разрозненный характер знаний, недостаточно правильные формулировки базовых понятий, нарушения логической последовательности в изложении программного материала, но при этом он владеет фрагментарно основными разделами учебной программы, необходимыми для дальнейшего обучения и может применять полученные знания по образцу в стандартной ситуации;
- оценка «неудовлетворительно (2)» выставляется студенту, который не знает большей части основного содержания учебной программы дисциплины, допускает грубые ошибки в формулировках основных понятий дисциплины и не умеет использовать полученные знания при решении типовых практических задач
- оценка «неудовлетворительно (1)» выставляется студенту, который не знает формулировок основных понятий дисциплины.

## 5. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности

Во время проведения дифференцированного зачета обучающиеся могут пользоваться программой дисциплины.