

**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>	Основы комбинаторики и теории чисел
<b>по направлению:</b>	Прикладная математика и информатика
<b>профиль подготовки:</b>	Математика
	Физтех-школа Прикладной Математики и Информатики
	кафедра дискретной математики
<b>курс:</b>	1
<b>квалификация:</b>	бакалавр

Семестры, формы промежуточной аттестации:

1 (осенний) - Экзамен

2 (весенний) - Экзамен

Аудиторных часов: 120 всего, в том числе:

лекции: 60 час.

семинары: 60 час.

лабораторные занятия: 0 час.

Самостоятельная работа: 90 час.

Подготовка к экзамену: 60 час.

Всего часов: 270, всего зач. ед.: 6

Количество контрольных работ, заданий: 2

Программу составил: А.М. Райгородский, д-р физ.-мат. наук, заведующий кафедрой

Программа обсуждена на заседании кафедры дискретной математики 01.06.2023

## Аннотация

Курс читается в первом году и служит весьма основательным введением как в теорию множеств, так и в комбинаторику, и в теорию чисел. Основная цель курса — заложить основу для изучения курсов дискретной математики, теории кодирования, криптографии и приложений в computer science, анализах сложных сетей, алгебры. При этом курс является неплохим введением в комбинаторику и теорию чисел, рассматривается несколько уникальных тем: теория обращения Мёбиуса, диаграммы Юнга, производящие функции, распределение простых чисел, приложения к геометрии чисел, начала аналитической теории чисел.

### 1. Цели и задачи

#### Цель дисциплины

- освоение основных современных методов экстремальной комбинаторики (ЭК): вероятностного метода, линейно-алгебраического метода, топологического метода.

#### Задачи дисциплины

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

### 2. Перечень формируемых компетенций

Освоение дисциплины направлено на формирование следующих компетенций:

Код и наименование компетенции	Индикаторы достижения компетенции
ОПК-1 Способен применять фундаментальные знания, полученные в области физико-математических и (или) естественных наук и использовать их в профессиональной деятельности	ОПК-1.2 Способен строить математические модели, производить количественные расчеты и оценки
ПК-1 Способен ставить, формализовывать и решать задачи, в том числе разрабатывать и исследовать математические модели изучаемых явлений и процессов, системно анализировать научные проблемы, получать новые научные результаты	ПК-1.2 Способен выдвигать гипотезы, строить математические модели для описания изучаемых явлений и процессов, оценивать качество разработанной модели

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

В результате освоения дисциплины обучающиеся должны

знать:

- фундаментальные понятия, законы, теории части дискретной математики – ЭК;
- современные проблемы соответствующих разделов дискретной математики (ЭК);
- понятия, аксиомы, методы доказательств и доказательства основных теорем в разделах, входящих в базовую часть цикла ЭК;
- основные свойства соответствующих математических объектов;
- аналитические и численные подходы и методы для решения типовых прикладных задач дискретной математики (ЭК).

уметь:

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

владеть:

- навыками освоения большого объема информации и решения задач ЭК ( 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 ЭК;
- предметным языком дискретной математики 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	Понятия множества и подмножества, простейшие операции над множествами. Упорядоченные пары и кортежи, декартово произведение	7	6		10
2	Основные правила комбинаторики: правило сложения, правило умножения, принцип Дирихле. Теорема о раскраске множества в два цвета. Оценки мощности множества попарно неортогональных $(-1,0,1)$ -векторов: верхняя оценка величиной 140 и нижняя оценка величиной 80 (задача)	8	8		10
3	Суммы, распространенные на делители числа. Функция Мёбиуса	7	8		10
4	Задачи о разбиениях чисел на слагаемые. Упорядоченные и неупорядоченные разбиения. Рекуррентные формулы. Количество всех упорядоченных разбиений на произвольные слагаемые. Диаграммы Юнга. Теоремы Эйлера о равенстве количеств неупорядоченных разбиений. Теорема о бесконечном произведении (б/д). Формула Харди–Рамануджана (б/д)	8	8		15
5	Основы теории делимости: наибольший общий делитель, наименьшее общее кратное, алгоритм Евклида. Функция Эйлера. Формула с произведением по простым числам.	7	6		15
6	Проблема Эрдеша–Гинзбурга–Зива. Теорема Лагранжа.	8	8		10
7	Простые числа. Показатели. Первообразные корни.	7	8		10
8	Теорема Дирихле о диофантовых приближениях: случай иррациональных чисел. Конечные цепные дроби	8	8		10

Итого часов	60	60		90
Подготовка к экзамену	60 час.			
Общая трудоёмкость	270 час., 6 зач.ед.			

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

##### Семестр: 1 (Осенний)

1. Понятия множества и подмножества, простейшие операции над множествами. Упорядоченные пары и кортежи, декартово произведение

Отображения и соответствия. Понятия образа и прообраза. Свойства отображений. Композиция и обратное отображение. Возведение множества в степень. Сравнение мощностей и понятие равномощности. Теорема Кантора—Бернштейна. Счётные и несчётные множества. Теорема Кантора. Отношения на множествах. Свойства бинарных отношений. Отношения эквивалентности, теорема о классах эквивалентности. Отношения частичного и линейного порядка. Минимальные/максимальные и наименьшие/наибольшие элементы. Свойства упорядоченных множеств. Операции над упорядоченными множествами. Изоморфизмы упорядоченных множеств.

2. Основные правила комбинаторики: правило сложения, правило умножения, принцип Дирихле. Теорема о раскраске множества в два цвета. Оценки мощности множества попарно неортогональных  $(-1,0,1)$ -векторов: верхняя оценка величиной 140 и нижняя оценка величиной 80 (задача)

Размещения, перестановки и сочетания. Формулы для чисел размещения и сочетания с повторениями и без повторений. Бином Ньютона, полиномиальная формула. Простейшие тождества (6 штук). Формулы для сумм степеней натуральных чисел. Формула включения и исключения. Знакопеременные тождества (2 штуки). Простые числа. Бесконечность множества простых. Основная теорема арифметики с доказательством.

3. Суммы, распространенные на делители числа. Функция Мёбиуса

Формула обращения Мёбиуса. Применение формулы обращения Мёбиуса для подсчета числа циклических последовательностей. Циклические последовательности с фиксированным количеством символов каждого типа (обязательное упражнение). Общая формула обращения Мёбиуса для частично упорядоченных множеств (б/д). Суммы по делителям и формула включений и исключений как частные случаи.

4. Задачи о разбиениях чисел на слагаемые. Упорядоченные и неупорядоченные разбиения. Рекуррентные формулы. Количество всех упорядоченных разбиений на произвольные слагаемые. Диаграммы Юнга. Теоремы Эйлера о равенстве количеств неупорядоченных разбиений. Теорема о бесконечном произведении (б/д). Формула Харди–Рамануджана (б/д)

Формальные степенные ряды, операции над ними, деление в столбик. Пример тождества, доказываемого с помощью формальных степенных рядов. Производящие функции. Теоремы о сходимости степенных рядов (б/д). Примеры, иллюстрирующие теоремы. Сходимость на границе интервала. Числа Фибоначчи и их производящая функция. Суммы чисел Фибоначчи, чисел сочетания и пр. Числа Каталана. Извлечение корней из степенных рядов. Формула для числа Каталана:  $d$ -во через производящие функции. Линейные рекуррентные соотношения с постоянными коэффициентами. Соотношения 1-ого порядка, в том числе неоднородные. Соотношения 2-ого порядка – с доказательством, соотношения большего порядка – только формулировка.

##### Семестр: 2 (Весенний)

5. Основы теории делимости: наибольший общий делитель, наименьшее общее кратное, алгоритм Евклида. Функция Эйлера. Формула с произведением по простым числам.

Основы теории сравнений. Системы вычетов. Теоремы Эйлера и Ферма (Ферма с двумя доказательствами). Значения некоторых биномиальных коэффициентов по данному модулю. Теорема Шевалле.

6. Проблема Эрдеша–Гинзбурга–Зива. Теорема Лагранжа.

Проблема Эрдеша–Гинзбурга–Зива. Решение проблемы при  $d=1$  и  $n=p$  (нижняя и верхняя оценки). «Почти решение» проблемы при  $d=2$  и  $n=p$  (нижняя и верхняя оценки). Теорема Лагранжа о числе корней многочлена по простому модулю. Теорема Вильсона. Китайская теорема об остатках. Сравнения второй степени по простому модулю. Квадратичные вычеты и невычеты. Символы Лежандра. Определение, простейшие свойства, формула для  $(2/p)$ . Квадратичный закон взаимности.

7. Простые числа. Показатели. Первообразные корни.

Показатели. Первообразные корни. Существование по модулю  $2, 4, p, p^a, 2p^a$ . Несуществование по другим модулям (можно рассказать идею без подробных выкладок). Индексы. Несколько слов об алгоритмических проблемах дискретного логарифмирования. Распределение простых чисел в натуральном ряде. Функции  $\pi(x)$ ,  $\theta(x)$ ,  $\psi(x)$ . Теорема о равенстве нижних и верхних пределов. Теорема Чебышёва. Асимптотический закон распределения простых (б/д). «Дырки» между соседними простыми числами (б/д).

8. Теорема Дирихле о диофантовых приближениях: случай иррациональных чисел. Конечные цепные дроби

Двумерная теорема Минковского. Ее уточнение для замкнутых множеств (б/д). Применение теоремы Минковского для передоказательства теоремы Дирихле. Конечные цепные дроби. Каноническая запись. Подходящие дроби. Бесконечные цепные дроби. Уточнение теоремы Дирихле (б/д). Зависимость качества аппроксимации от скорости роста неполных частных: существование чисел с заданным наперед качеством аппроксимации; золотое сечение как самое плохо приближаемое число (б/д). Теорема о периодичности дроби для квадратичной иррациональности (доказательство в одну сторону).

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

Учебная аудитория, оснащенная компьютером и мультимедийным оборудованием (проектор, звуковая система).

## **6. Перечень рекомендуемой литературы**

### **Основная литература**

1. Основы комбинаторики и теории чисел : сборник задач, учебное пособие для вузов / А. А. Глибичук, Д. Г. Ильинский, Д. В. Мусатов [и др.]. — Долгопрудный, Интеллект, 2019.— URL: <http://books.mipt.ru/book/301289> (дата обращения: 17.12.2020). - Полный текст (Режим доступа : из сети МФТИ / Удаленный доступ)
2. Линейно-алгебраический метод в комбинаторике [Текст] : [учеб. пособие для вузов] / А. М. Райгородский .— М. : МЦНМО, 2007 .— 136 с.

### **Дополнительная литература**

1. Комбинаторика и теория вероятностей [Текст] : [учеб. пособие для вузов] / А. М. Райгородский .— Долгопрудный : Интеллект, 2013 .— 104 с.

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

Не используются

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

Не предусмотрено.

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

Рекомендуется успешно сдавать контрольные работы, так как это упрощает итоговую аттестацию по предмету.

Для подготовки к итоговой аттестации по предмету лучше всего пользоваться материалами лекций.

**ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)**

**по направлению:** Прикладная математика и информатика  
**профиль подготовки:** Математика  
Физтех-школа Прикладной Математики и Информатики  
кафедра дискретной математики  
**курс:** 1  
**квалификация:** бакалавр

Семестры, формы промежуточной аттестации:

1 (осенний) - Экзамен  
2 (весенний) - Экзамен

**Разработчик:** А.М. Райгородский, д-р физ.-мат. наук, заведующий кафедрой

## 1. Компетенции, формируемые в процессе изучения дисциплины

Код и наименование компетенции	Индикаторы достижения компетенции
ОПК-1 Способен применять фундаментальные знания, полученные в области физико-математических и (или) естественных наук и использовать их в профессиональной деятельности	ОПК-1.2 Способен строить математические модели, производить количественные расчеты и оценки
ПК-1 Способен ставить, формализовывать и решать задачи, в том числе разрабатывать и исследовать математические модели изучаемых явлений и процессов, системно анализировать научные проблемы, получать новые научные результаты	ПК-1.2 Способен выдвигать гипотезы, строить математические модели для описания изучаемых явлений и процессов, оценивать качество разработанной модели

## 2. Показатели оценивания компетенций

В результате изучения дисциплины «Основы комбинаторики и теории чисел» обучающийся должен:

### знать:

- фундаментальные понятия, законы, теории части дискретной математики – ЭК;
- современные проблемы соответствующих разделов дискретной математики (ЭК);
- понятия, аксиомы, методы доказательств и доказательства основных теорем в разделах, входящих в базовую часть цикла ЭК;
- основные свойства соответствующих математических объектов;
- аналитические и численные подходы и методы для решения типовых прикладных задач дискретной математики (ЭК).

### уметь:

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

### владеть:

- навыками освоения большого объема информации и решения задач ЭК ( 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 ЭК;
- предметным языком дискретной математики и навыками грамотного описания решения задач и представления полученных результатов.

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

Примерный вариант контрольной работы приведен в конце программы отдельным файлом.

Тема для курсовой:

- Докажите, что объединение двух счётных множеств счётно.

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

Полный список вопросов к экзаменам и правила сдачи экзаменов приведены в отдельных файлах в конце рабочей программы.

Примерные вопросы к экзамену:

- Приведите пример соответствия, которое обладает следующими свойствами: а) сюръективное, не инъективное, не отображение; б) не сюръективное, инъективное, не отображение; в) не сюръективное, не инъективное, отображение.
- Сформулируйте определяющие свойства соответствий, обратных к инъективным и к сюръективным.
- Соответствие является одновременно инъективным и сюръективным. Обязательно ли оно является биекцией?
- Докажите, что композиция отображений, инъективных соответствий, сюръективных соответствий и биекций является отображением, инъективным соответствием, сюръективным соответствием, биекцией соответственно.
- Покажите, что в любом бесконечном множестве найдётся счётное подмножество.
- Докажите, что любое подмножество счётного множества не более чем счётно.

Билет 1:

1. Сформулируйте определяющие свойства соответствий, обратных к инъективным и к сюръективным.
2. Соответствие является одновременно инъективным и сюръективным. Обязательно ли оно является биекцией?

Билет 2:

1. Докажите, что композиция отображений, инъективных соответствий, сюръективных соответствий и биекций является отображением, инъективным соответствием, сюръективным соответствием, биекцией соответственно.
2. Покажите, что в любом бесконечном множестве найдётся счётное подмножество.

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;

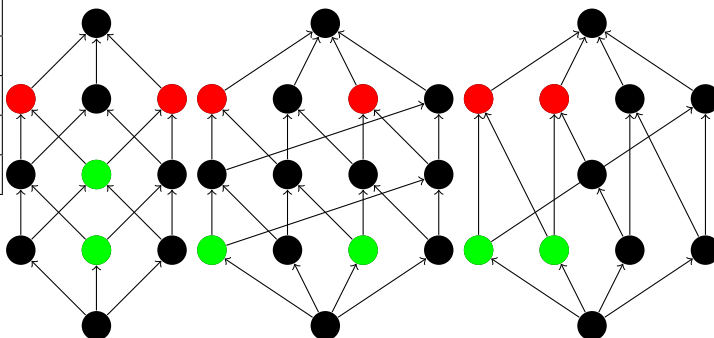
- оценка «удовлетворительно (3)» выставляется студенту, показавшему фрагментарный, разрозненный характер знаний, недостаточно правильные формулировки базовых понятий, нарушения логической последовательности в изложении программного материала, но при этом он владеет фрагментарно основными разделами учебной 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 экзамена обучающиеся могут пользоваться программой дисциплины.

1. Справа нарисованы диаграммы Хассе частично упорядоченных множеств  $A_1, A_2, A_3$ . Заполните таблицу, указав плюсом верные утверждения, а минусом — неверные.

ч.у.м. $A =$	$A_1$	$A_2$	$A_3$
решётка	нет	нет	нет
полная решётка	нет	нет	нет
$\vee$ -полурешётка	нет	нет	нет
$\wedge$ -полурешётка	нет	нет	нет



Комментарий: У зеленых элементов нет  $\sup$ , у красных —  $\inf$ .

2. На картинках справа описаны отношения  $R_1, R_2, R_3$ . Заполните таблицу, указав плюсом верные утверждения, а минусом — неверные.

отношение $R$	$R_1$	$R_2$	$R_3$
$R$ предпорядок	нет	да	нет
$R$ полный предпорядок	нет	нет	нет
$R$ квазитранзитивно	нет	да	нет
$R$ ациклично	да	да	да
$R$ решётка	нет	нет	нет
$R$ полная решётка	нет	нет	нет

Решение:  $R_1: 3 \prec 4 \prec 5$  — все отношения  $\prec$ , поэтому квазитранзитивности нет (должно было быть  $3 \prec 5$ ), ацикличность есть.

$R_2$ : это отношение эквивалентности, то есть предпорядок, но не полный.

$R_3: 2 \prec 3, 3 \prec 1, 1 \prec 5, 5 \prec 4$  — все отношения  $\prec$ , поэтому квазитранзитивности нет, ацикличность есть.

3. (2018-2) В мешке имеется 20 чёрных, 15 белых, 10 синих и 20 красных носков. Какое минимальное количество носков необходимо вытащить, чтобы среди них гарантированно нашлось ...

5 носков одного цвета

4 чёрных носка

2 носка одного цвета и 2 носка другого цвета

по одному носку каждого из цветов

4. (2017-2) Запишите только ответы в пустые клетки (разрешается использовать факториалы и символы  $C_*, A_*, P(*, \dots, *)$ ). Имеется 15 студентов. Количество способов ...

выделить 2 участников олимпиады по математике и 3 участников олимпиады по программированию (один студент может участвовать в нескольких олимпиадах) равно

разбить их на три команды (белую, синюю и красную) по 5 студентов равно

разбить их на пять групп по 3 студента (группы неразличимы) равно

разбить их на три пары и две тройки равно

$$\frac{1}{3!} \frac{1}{2!} P(2, 2, 2, 3, 3)$$

5. (2017-4) В кинотеатре 7 рядов по 10 мест каждый. Группа из  $N$  студентов сходилa на утренний сеанс, а потом на вечерний. При каком наименьшем  $N$  при любой рассадке студентов в кинотеатре найдутся двое студентов, которые на утреннем сеансе сидели в одном ряду и на вечернем тоже сидели в одном ряду?

Решение:  $N = 50$ . Если студентов 49, то можно их рассадить 7 по 7 человек так, чтобы условие не было выполнено (во второй раз можно посадить так, чтобы в каждом ряду сидели студенты из разных рядов утреннего сеанса). Если студентов 50, то в вечернем сеансе найдётся ряд, на котором сидит  $\geq \frac{50}{7}$  студентов, то есть 8 студентов. По принципу Дирихле, двое из этих восьми сидели утром в одном ряду.

6. (2017-3) Сколько пятизначных чисел не имеют в своей десятичной записи одинаковых подряд идущих цифр? (К примеру, не подходят 14388, 22259, 32336.)

Решение: Для первой цифры есть 9 вариантов (от 1 до 9), для второй 9 вариантов (отлична от 1-й), для третьей 9 вариантов (отлична от 2-й), ... . Итого получаем  $9^5$  вариантов.

7. (2018-4)

Пусть на оси абсцисс размещено  $N$  точек. *Дуговой диаграммой типа*  $(n_1, \dots, n_k)$  (где  $n_1 + \dots + n_k = N$ ) назовём картинку, на которой точки разбиты на подмножества из  $n_1, n_2, \dots, n_k$  элементов и в каждом из подмножеств последовательно соединены дугами. Сколько существует различных дуговых диаграмм типа, соответствующего изображенному на картинке справа? В ответе не допускается использование символов  $C^*, A^*$ , знаков  $\sum$  и троеточий.



Решение: на картинке изображена диаграмма типа  $(3, 3, 3, 2)$ . Количество способов разбить множество из 11 элементов на подмножества указанной мощности равно  $\frac{1}{3!} P(3; 3; 3; 2) = \frac{11!}{(3!)^4 \cdot 2!}$ .

8. Приведите пример решетки, которая не является полной решеткой.

Решение: Возьмём, например,  $\langle \mathbb{N}, \cdot \rangle$ : решётка (доказывали на семинаре), у всего множества  $\mathbb{N}$  нет  $\sup$  (нет числа, которое делится на все простые), поэтому это не полная решётка.

9. В каждой конечной решётке есть наименьший/наибольший элемент.

Решение: Докажем для наименьшего (для наибольшего аналогично). В любом конечном ч.у.м.е есть минимальный элемент. Если он единственный, то он наименьший. Если есть два минимальных элемента  $x, y$ , то у пары  $x, y$  есть  $\inf(x, y) \leq x, y$ , откуда  $x = \inf(x, y) = y$  (из минимальности).

для получения оценки удовл. (3-4) надо знать вопросы на удовл. и основные определения и формулировки утверждений курса. «Знать» означает умение подготовить и обсудить любой вопрос на удовл. с преподавателем за **20** минут. Если вы не можете ответить на какой-то вопрос, вы гарантированно получите не больше удовл.(3). Критерий на "двойку" приведён в отдельном списке в конце.

Оценка хор. (5-7): знать вопросы на удовл. и хор., а также основные определения и формулировки утверждений курса. Вопросы на удовл. надо уметь отвечать за **15** минут, вопросы на хор. за **20** минут. Если вы не можете ответить на какой-то вопрос, вы гарантированно получите не больше хор.(5). Разница между 5,6 и 7 заключается в точности ответа, и во времени, потраченном на ответ на вопросы.

Оценка отл. (8-10): знать все вопросы, а также основные определения и формулировки утверждений курса. Вопросы на удовл. надо уметь отвечать за **10** минут, вопросы на хор. за **15** минут, вопросы на отл. **20** минут. Если вы не можете ответить на какой-то вопрос, вы гарантированно получите не больше отл.(8). Для получения оценки отл.(9-10) даются дополнительные задачи на размышление.

### Вопросы

В вопросах даны номера задач из листков, которые предполагается рассказывать в билете или указание на точную формулировку. На экзамене будет такая же формулировка, т.е. предполагается, что вы запомните условия задач.

При ответе на вопросы билетов без доказательства можно пользоваться следующими утверждениями. Вы должны уметь приводить соответствующие формулировки.

Основная Теорема Арифметики

Теорема о радиусе сходимости формального степенного ряда.

Формула  $(1+x)^\alpha = \sum_{n=0}^{\infty} \binom{\alpha}{n} t^n$  для  $\alpha \in \mathbb{Q} \setminus \mathbb{N}$ .

Формула обращения Мёбиуса для ч.у.м.

Лемма о  $3r$  векторах (для док-ва теоремы Эрдеша-Гинзбурга-Зива).

### Вопросы на удовл.

1. Задание множества перечислением и определяющим свойством. Отношение подмножества и его свойства: рефлексивность, антисимметричность, транзитивность. Равенство множеств. Парадокс Рассела.
2. Операции над множествами: объединение, пересечение, разность, симметрическая разность, дополнение. Тождества: коммутативность, ассоциативность, дистрибутивность, законы де Моргана. Доказательства при помощи диаграмм Эйлера и непосредственные.
3. Упорядоченные пары и кортежи. Декартово произведение и декартова степень. Их свойства. (Задачи 1.9a)б) и 1.11a)б))
4. Понятие соответствия. Понятие отображения. Обозначения. Инъективные и сюръективные соответствия. Инъекции и сюръекции. Биекции. Взаимно однозначные отображения. Утверждение о том, что соответствие является биекцией тогда и только тогда, когда оно само и обратное к нему являются отображениями.
5. Понятия образа и прообраза множества при соответствии. Критерий равенства образа пересечения и пересечения образов. Аналогичные критерии с объединением и разностью.
6. Область определения и область значений соответствия. Сужение и продолжение соответствия. Композиция соответствий, её ассоциативность.
7. Количество элементов в конечном множестве. Корректность определения. Равномощность множеств. Счётные множества. Счётное объединение счётных множеств счётно.
8. Докажите, что если  $A$  бесконечно, а  $B$  не более чем счётно, то  $A \cup B \cong A$ . Континуальные множества. Доказательство того, что отрезок, полуинтервал, интервал континуальны.
9. Теорема Кантора для счётных множеств.
10. Отношения на множествах. Свойства бинарных отношений. Отношения эквивалентности, теорема о классах эквивалентности. Отношения частичного и линейного порядков, предпорядка. Примеры отношений (задача 5.1 и 5.5).
11. Частично упорядоченные множества. Диаграмма Хассе. Гомоморфизмы и изоморфизмы. Описание попарно неизоморфных ч.у.м. для 3 и 4 элементов. Минимальные, максимальные, наибольшие и наименьшие элементы. Их свойства (на примере задачи 5.8).
12. Предпорядки: определение и примеры (задача 6.6). Полный предпорядок. Построение по предпорядку отношения безразличия и индуцированного порядка на классах эквивалентности. Равносильность полноты предпорядка и линейности индуцированного порядка.

13. Решётки, полные решётки, полурешётки. Примеры (задача 7.10).
14. Правило сложения. Правило умножения. Примеры: автомобильные номера, количество шестизначных чисел с различными цифрами (задача 8.5). Принцип Дирихле. Пример на принцип Дирихле с квадратом.
15. Размещения, перестановки и сочетания: определение как теоретико-множественных объектов. Доказательство формул для чисел размещения и сочетания с повторениями и без повторений. Типовые задачи (аналогичные 8.7, 8.9, 8.10, 8.11).
16. Бином Ньютона. Полиномиальный коэффициент и полиномиальная формула. Типовые задачи в духе: сколько имеется способов раздать 11 разных цветков, трём девушкам: какой-то — 5, а остальным — по 3 цветка?
17. Комбинаторные тождества (6 штук).
18. Формула включений и исключений (формулировка и док-во для  $n = 3$ ). Формула для количества беспорядков на  $n$  элементах (Задача 9.19 про перестановки книг).
19. Формула включений и исключений (формулировка и док-во для  $n = 3$ ). Формула для количества сюръекций из  $k$ -элементного множества в  $m$ -элементное (Задача 9.20 про домики).
20. Функция Мёбиуса. Сумма значений функции Мёбиуса по делителям числа, а также по делителям числа, содержащим в разложении чётное количество простых сомножителей (Задача 10.1).
21. Операция циклического сдвига на линейных последовательностях. Период линейной последовательности. Свойства периода. Общий вид последовательности периода  $d$  и длины  $n$ .
22. Задачи о разбиениях чисел на слагаемые. Упорядоченные разбиения. Количество всех упорядоченных разбиений на произвольные слагаемые.
23. Диаграммы Юнга. Теоремы Эйлера о равенстве количеств неупорядоченных разбиений (3 штуки). Формула Харди–Рамануджана (б/д).
24. Линейные рекуррентные соотношения с постоянными коэффициентами. Характеристическое уравнение. Общая формула для соотношения  $n$ -го порядка (формулировка, частный случай  $n = 2$ ). Формула для чисел Фибоначчи.
25. Формальные степенные ряды, операции над ними. Определение обратного ряда. Пример деления в столбик. Примеры нахождения обратных рядов (задача 13.6).
26. Числа Фибоначчи и их производящая функция. Радиус сходимости, значение  $\sum_{n=0}^{\infty} \frac{F_n}{2^n}$ .
27. Числа Каталана (определение через пары скобочных последовательностей). Рекуррентное соотношение для чисел Каталана.
28. Числа Каталана. Производящая функция для чисел Каталана.
29. Проблема Эрдеша–Гинзбурга–Зива. Контрпримеры для  $d = 1, 2$ . История проблемы.

#### Вопросы на хор.

30. Возведение множества в степень другого множества. Булеан. Свойства возведения множества в степень:  $A^B \times A^C \cong A^{B \cup C}$  (для непересекающихся  $B$  и  $C$ );  $A^C \times B^C \cong (A \times B)^C$ ;  $(A^B)^C \cong A^{B \times C}$  (для произвольных  $A, B, C$ ).
31. Теорема Кантора для произвольных множеств.
32. Континуальность множества  $2^{\mathbb{N}}$ .
33. Континуальность плоскости, трёхмерного пространства,  $n$ -мерного пространства  $\mathbb{R}^k$  и счётного пространства  $\mathbb{R}^{\mathbb{N}}$ . Формулировка континуум-гипотезы.
34. Сумма, произведение и декартово произведение частично упорядоченных множеств. Свойства операций: ассоциативность, (не)коммутативность, (не)дистрибутивность. Может ли линейно упорядоченное множество  $A$ , в котором больше одного элемента, быть изоморфным а)  $A + A$ ? б)  $A \cdot A$ ? Какие из следующих множеств изоморфны:  $\mathbb{Q} \cdot \mathbb{Z}$ ,  $\mathbb{Z} \cdot \mathbb{Q}$ ,  $\mathbb{Q} \cdot \mathbb{Z} \cdot \mathbb{Q}$ ? Теоремой об изоморфизме можно пользоваться без доказательства.
35. Агрегирование предпорядков по большинству и консенсусом. Теорема о представлении любого полного отношения как агрегирования по большинству линейных порядков. Теорема о представлении любого предпорядка как агрегирования консенсусом полных предпорядков.
36. Квазитранзитивные и ациклические отношения. Свойства и примеры (задачи 7.5–7.8).
37. Решётки, полные решётки, полурешётки. Примеры (задача 7.10). Свойства решёток (задача 7.13).
38. Теорема о раскраске множества в два цвета.
39. Формула включений и исключений.
40. Формула включений и исключений (формулировка и док-во для  $n = 3$ ). Формула для функции Эйлера через произведение по простым сомножителям (док-во через формулу вкл-искл.)

41. Сумма степеней натуральных чисел. Знакопеременные тождества (2 штуки).
42. Формула обращения Мёбиуса.
43. Функция Эйлера. Формула с произведением по простым числам: доказательство при помощи формулы обращения Мёбиуса.
44. Операция циклического сдвига на линейных последовательностях. Период линейной последовательности. Свойства периода (б/д). Явная формула для числа циклических последовательностей для частных случаев ( $n = 3, 4, 5, 6$ ) (задача 10.5).
45. Функция Мёбиуса на ч.у.м. Вычисление функции Мёбиуса на примере пятиэлементного множества (задача 11.1). Функция Мёбиуса на ч.у.м.е  $\langle \mathbb{N}, \leq \rangle$  (задача 11.4). Общая формула обращения Мёбиуса для частично упорядоченных множеств (б/д), её применение к задаче 11.4.
46. Функция Мёбиуса на ч.у.м. Совпадение функции Мёбиуса  $\mu(1, n)$  на ч.у.м.  $\langle \mathbb{N}, : \rangle$  и обычной функции Мёбиуса  $\mu(n)$  на  $\mathbb{N}$  (для всех  $n$ ). Общая формула обращения Мёбиуса для частично упорядоченных множеств (б/д).
47. Задачи о разбиениях чисел на слагаемые. Упорядоченные и неупорядоченные разбиения. Рекуррентные формулы.
48. Линейные рекуррентные соотношения с постоянными коэффициентами. Характеристическое уравнение. Общая формула для соотношения 2-го порядка с различными корнями характеристического уравнения.
49. Линейные рекуррентные соотношения с постоянными коэффициентами. Характеристическое уравнение. Общая формула для соотношения 2-го порядка с совпадающими корнями характеристического уравнения.
50. Формальные степенные ряды, операции над ними. Определение обратного ряда. Критерий обратимости ряда (задача 13.5). Примеры нахождения обратных рядов (задача 13.6).
51. Формальные степенные ряды, операции над ними. Определение обратного ряда. Пример деления в столбик. Комбинаторное тождество, получаемое с использованием формального степенного ряда  $\frac{1}{(1-x^2)^2}$ .
52. Числа Каталана. Формула для коэффициентов ряда  $\sqrt{1+x}$  (б/д). Вывод из неё формулы для чисел Каталана.
53. Определение радиуса сходимости формального степенного ряда. Теорема о сходимости степенных рядов (формулировка). Примеры, иллюстрирующие теорему (задача 14.2: 3 примера, показывающие, что на границе может быть сходимость/расходимость).

#### Вопросы на отл.

54. Теорема Кантора–Бернштейна.
55. Плотный порядок. Изоморфизм счётных плотных линейно упорядоченных множеств без наибольшего и наименьшего элементов.
56. Принцип Дирихле. Оценки мощности множества попарно неортогональных  $(-1, 0, 1)$ -векторов: верхняя оценка величиной 140 и нижняя оценка величиной 70.
57. Формула включений и исключений. Применение формулы для вывода формулы для функции Эйлера, числа беспорядков и количества сюръективных отображений.
58. Применение формулы обращения Мёбиуса для подсчёта числа циклических последовательностей.
59. Передоказательство формулы включений и исключений при помощи формулы обращения Мёбиуса на ч.у.м. Определение множества  $X$ , порядка  $\preceq$ . Вычисление функции Мёбиуса на данном ч.у.м.
60. Передоказательство формулы включений и исключений при помощи формулы обращения Мёбиуса на ч.у.м. Определение множества  $X$ , порядка  $\preceq$ , функции  $f, g$ . Формула для вычисления функции Мёбиуса на данном ч.у.м. (б/д). Вывод формулы включений и исключений.
61. Производящая функция для количества неупорядоченных разбиений в общем виде и для разбиений специального вида (задача 14.10). Доказательство того, что количества разбиений на попарно различные слагаемые и на нечётные слагаемые совпадают.
62. Числа Каталана. Определение через пары скобочных последовательностей. Вывод формулы при помощи производящей функции.
63. Проблема Эрдеша–Гинзбурга–Зива (общая формулировка). Контрпримеры при  $d = 1, 2$ . Тождества с биномиальными коэффициентами ( $C_{2p-1}^p \equiv 1 \pmod{p}$ ,  $C_{2p-1-q}^{p-q} \equiv 0 \pmod{p}$ , если  $q \in \{1, 2, \dots, p-1\}$ ).
64. Решение проблемы Эрдеша–Гинзбурга–Зива для  $d = 1$ ,  $n = p$ . Формулами  $C_{2p-1}^p \equiv 1 \pmod{p}$ ,  $C_{2p-1-q}^{p-q} \equiv 0 \pmod{p}$ , если  $q \in \{1, 2, \dots, p-1\}$ , можно пользоваться без доказательства.

**65.** Проблема Эрдеша–Гинзбурга–Зива при  $d = 2$  и  $n = p$ : нижняя и верхние оценки (формулировка).  
Формулировка основной леммы. Вывод из неё теоремы Роньяи.

### Вопросы на «двойку»

Для того, чтобы получить на экзамене удовл.(3), необходимо продемонстрировать умение давать формулировки и понимание всех определений из курса, а также доказательство основных и простейших фактов из курса. Продемонстрировать — значит уметь за 5 минут привести формулировку и за 15 минут подготовить и рассказать преподавателю доказательство факта (вне зависимости от того, было ли это рассказано на лекции или нет). В частности, за незнание хотя бы двух пунктов из следующего списка студент будет отправлен на пересдачу.

Все утверждения, про которые не указано «(формулировка)», необходимо уметь и формулировать, и доказывать.

- Отношение «быть подмножеством» и его свойства: рефлексивность, антисимметричность, транзитивность.
- Операции над множествами: объединение, пересечение, разность, симметрическая разность, дополнение.
- Тождества: коммутативность, ассоциативность, дистрибутивность, законы де Моргана.
- Умение иллюстрировать/доказывать тождества при помощи диаграмм Эйлера/непосредственным способом.
- Определение упорядоченных пар и кортежей, декартова произведения и декартовой степени.
- Определение соответствия, отображения, инъективных и сюръективных соответствий, инъекции, сюръекции, биекции.
- Понятия равномощности множеств.
- Понятие счётного множества (определение, и примеры: чётные числа, целые числа).
- Счётное объединение счётных множеств счётно.
- Счётность множества рациональных чисел.
- Теорема Кантора для счётных множеств.
- Утверждение о том, что если  $A$  бесконечно, а  $B$  не более чем счётно, то  $A \cup B \cong A$ .
- Определение отношения эквивалентности.
- Определение классов эквивалентности.
- Определения отношений нестрогого частичного порядка, линейного порядка, плотного порядка.
- Определение изоморфизма упорядоченных множеств.
- Минимальные/максимальные и наименьшие/наибольшие элементы в упорядоченном множестве.
- Правила сложения и умножения в комбинаторике.
- Принцип Дирихле.
- Теорема о раскраске множества в два цвета (формулировка проблемы).
- Размещения, перестановки и сочетания (определения и умение решать задачи вроде: *Сколько способами из 4 разных школьников можно выбрать двоих для дежурства?*).
- Формулы для чисел размещений и сочетаний с повторениями и без повторений.
- Бином Ньютона.

- Полиномиальная формула.

- Для каждого  $n \in \mathbb{N}$  найдите суммы:

$$\begin{aligned} C_n^0 + C_n^1 + \dots + C_n^n, \\ C_n^0 - C_n^1 + \dots + (-1)^n C_n^n, \\ (C_n^0)^2 + (C_n^1)^2 + \dots + (C_n^n)^2. \end{aligned}$$

- Формула включений и исключений (формулировка и доказательство для  $n = 3$ ).
- Определение функции Мёбиуса.
- Формула для суммы функции Мёбиуса по делителям.
- Формула обращения Мёбиуса(формулировка).
- Операция циклического сдвига на линейных последовательностях.
- Определение периода линейной последовательности. Утверждение о том, что период последовательности делит его длину.
- Формула для подсчёта числа циклических последовательностей (формулировка).
- Упорядоченные и неупорядоченные разбиения.
- Количество всех упорядоченных разбиений на произвольные слагаемые.
- Диаграммы Юнга.
- Три теоремы Эйлера о равенстве количеств неупорядоченных разбиений.
- Определение функции Мёбиуса на ч.у.м.
- Определения формального степенного ряда, сложения и умножения рядов.
- Определение чисел Фибоначчи. Формула для чисел Фибоначчи через сумму двух геометрических прогрессий.
- Определение линейного рекуррентного соотношения и его характеристического уравнения.
- Теоремы о формуле для последовательностей, заданных рекуррентным соотношением 2-го порядка (формулировка).
- Определение радиуса сходимости формального степенного ряда. Теорема о сходимости степенных рядов (формулировка). Радиус сходимости производящей функции чисел Фибоначчи.
- Определение производящей функции последовательности.
- Производящая функция для чисел Фибоначчи, Каталана (вид без бесконечной суммы).
- Определение чисел Каталана.
- Рекуррентное соотношения для чисел Каталана.

**Порядок проведения экзамена**

На экзамене каждый студент получит 6-7 вопросов разной сложности (сложность зависит от рейтинга студента).

На ответ на все вопросы даётся 1 час. В ответе на вопрос надо быстро сформулировать определения и идеи, встречающиеся в доказательстве утверждений. Экзаменатор может задать уточняющий/дополнительный вопрос по билету/доказательству.

Критерии оценки:

для получения оценки удовл. (3-4) надо знать вопросы на удовл. и основные определения и формулировки утверждений курса. В ходе экзамена необходимо будет ответить на 6 или 7 вопросов на удовл. или больше. Если вы не знаете хотя бы двух вопросов из списка на удовл., вам ставится неуд.(2). Разница между 3 и 4 определяется скоростью ответа на эти вопросы, и в спорных случаях дополнительным вопросом преподавателя.

Оценка хор. (5-6) : знать вопросы на удовл. и хор., а также основные определения и формулировки утверждений курса. В ходе экзамена необходимо будет ответить на 4 вопроса на хор. или больше. Если вы не знаете одного вопроса из списка на хор., ставится не больше хор(5). Если вы не знаете трёх вопросов на хор., ставится не больше удовл. (4). Разница между хор.(5) и хор.(6) определяется скоростью ответа на вопросы на хор. и дополнительным вопросом преподавателя. Хор.(7) ставится, если вы знаете вопросы на хор., и можете рассказать половину вопросов на отл.

Оценка отл. (8-9) : знать все вопросы, а также основные определения и формулировки утверждений курса. В ходе экзамена необходимо ответить на 3 вопроса на отл. Если вы не знаете двух вопросов на отл., то ставится хор.(7)

На отл(10) может быть задана дополнительная задача.

**Итоговая оценка**

Если  $S$  — оценка в семестре, а  $E$  — оценка за экзамен, то итоговая оценка  $I$  равна

$$I = \begin{cases} 2, & E = 2 \\ \max(3, \min(4, [0.5 \cdot E + 0.5 \cdot S + 0.5])), & E = 3, 4 \\ \max(5, \min(7, [0.5 \cdot E + 0.5 \cdot S + 0.5])), & E = 5, 6, 7 \\ \max(8, \min(10, [0.5 \cdot E + 0.5 \cdot S + 0.5])), & E = 8, 9, 10 \end{cases},$$

где  $[x]$  — целая часть  $x$ .

**Порядок проведения пересдачи**

Если на экзамене вы получили оценку неуд.(2), то на пересдаче вы получаете 5 вопросов из списка «на тройку».

- если вы ответите на все вопросы «быстро» (менее, чем за 50 минут), то получаете дополнительные вопросы на удовл.(4), хор.(5), и.т.д.

- если вы ответите на все вопросы «нормально», т.е. менее чем на 1 час 15 минут, то получаете два дополнительных вопроса «на тройку», ответив на которые быстрее, чем за полчаса, получите удовл.(3).

- если вы не ответите хотя бы один вопрос полностью, преподаватель может задать 1-2 дополнительных вопроса на смежные темы (по правилам, если вы хотя бы на два вопроса из списка «на тройку» не ответите, то получите неуд.(2)).

**Вопросы на удовл.**

1. Простые числа. Основная теорема арифметики (формулировка, существование).
2. Основы теории делимости: наибольший общий делитель, наименьшее общее кратное, алгоритм Евклида (доказательство того, что алгоритм остановится, и последний ненулевой член — это НОД).
3. Представимость наибольшего общего делителя  $(a, b)$  в виде линейной целочисленной комбинации  $a$  и  $b$ .
4. Лемма Евклида: формулировка, любое из доказательств, не использующее основную теорему арифметики.
5. Вывод единственности в основной теореме арифметики через лемму Евклида.
6. Основы теории сравнений. Системы вычетов. Определение сложения и умножения. Обратимые элементы. Делители нуля. Связь между ними.
7. Системы вычетов. Малая теорема Ферма (любое доказательство).
8. Системы вычетов. Теорема Эйлера.
9. Теорема Лагранжа о числе корней многочлена по простому модулю(б/д). Теорема Вильсона (с использованием теоремы Лагранжа).

10. Доказательство теоремы Вильсона с использованием первообразных корней.
11. Бесконечность количество простых вида  $3k + 2$ ,  $4k + 3$ ,  $4k + 1$ .
12. Сравнения второй степени. Квадратичные вычеты и невычеты. Количество вычетов и невычетов по простому нечётному модулю  $p$ .
13. Квадратичные вычеты и невычеты. Символ Лежандра. Формулы  $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}}$ ,  

$$\left(\frac{a_1 \dots a_n}{p}\right) = \left(\frac{a_1}{p}\right) \dots \left(\frac{a_n}{p}\right).$$
14. (умение) Умение вычислить символ Лежандра.
15. Матрицы Адамара. Определение. Нормальная форма. Не очень конкретные разговоры про связь с теорией кодов, исправляющих ошибки, и с задачей про  $-1, 0, 1$  с первой лекции.
16. Существование матриц при  $n = 1$  и  $2$ . Необходимость делимости на  $4$  при  $n > 3$ . Гипотеза Адамара. Общие слова про недоказанность.
17. Попытка построить матрицу для  $n = 2^k$  путем наложения единиц на минус единицы (получается только  $k$  строчек). Решение для  $n = 2^k$ .
18. Показатель. Показатель элемента из множества  $\mathbb{Z}_m$  делит  $\varphi(m)$ . Первообразный корень (определение и значения при  $m \leq 7$ ). Пример модуля, по которому не существует первообразного корня.
19. Индексы. Таблицы индексов. Решение степенных сравнений (умение).
20. Теорема Дирихле о диофантовых приближениях (формулировка и доказательство любым способом).
21. Рекуррентные соотношения для числителей и знаменателей подходящих дробей.
22. Конечные цепные дроби. Каноническая запись. Подходящие дроби. Рекуррентные соотношения для числителей и знаменателей подходящих дробей (б/д). Следствия: несократимость подходящих дробей, возрастание подходящих дробей с четными номерами и убывание подходящих дробей с нечетными номерами.
23. Определение бесконечной цепной дроби. Доказательство сходимости соответствующих подходящих цепных дробей (можно пользоваться без доказательства соотношениями на их коэффициенты).
24. Бесконечные периодические цепные дроби. Теорема о периодичности дроби для квадратичной иррациональности (доказательство в одну сторону). Умение находить периодическую цепную дробь по её значению, и наоборот, нахождение значения дроби по её периоду.
25. Квадратичные иррациональности. Множество  $\mathbb{Z}[\sqrt{m}]$ : сопряжение, замкнутость сложения, умножения. Согласованность сопряжения и умножения. Норма и её свойства.
26. Пара  $(a, b)$ , где  $a + b\sqrt{2} = (1 + \sqrt{2})^n$  является решением уравнения Пелля  $a^2 - 2b^2 = \pm 1$ .
27. Связь между решениями уравнения Пелля  $a^2 - 2b^2 = \pm 1$  и элементами  $\mathbb{Z}[\sqrt{2}]$  нормой  $1$ .
28. Определение равномерной распределённой последовательности по модулю  $1$ . Является ли  $\sqrt{n}$  р.р.  $(\text{mod } 1)$  последовательностью?
29. Определение равномерной распределённой последовательности по модулю  $1$ . Является ли р.р.  $(\text{mod } 1)$  последовательность  $a^n$  при  $a < 1$ ?
30. Определение всюду плотности. Последовательность  $\ln n$  всюду плотна на  $[0, 1]$ .
31. Определение всюду плотности. Если последовательность равномерно распределена по модулю  $1$ , то она и всюду плотна.
32. Тригонометрические суммы. Критерий Вейля для р.р.  $(\text{mod } 1)$  (формулировка). Последовательность  $\alpha n$  при иррациональном  $\alpha$  является р.р.  $(\text{mod } 1)$ . Что происходит при рациональном  $\alpha$ ?
33. Определение равномерной распределённой последовательности по модулю  $1$ . Являются ли р.р.  $(\text{mod } 1)$  последовательности а)  $1, \frac{1}{2}, \frac{1}{3}, \frac{2}{3}, \frac{1}{4}, \frac{2}{4}, \frac{3}{4}, \dots$ ; б)  $\frac{1}{2}, \frac{1}{4}, \frac{3}{4}, \frac{1}{8}, \frac{3}{8}, \frac{5}{8}, \frac{7}{8}, \frac{1}{16}, \frac{3}{16}, \frac{5}{16}, \frac{7}{16}, \frac{9}{16}, \frac{11}{16}, \frac{13}{16}, \frac{15}{16}, \dots$
34. Определение равномерной распределённой последовательности по модулю  $1$ . Пусть последовательность  $x_n$  р.р.  $(\text{mod } 1)$  и  $m$  — фиксированное целое число, не равное нулю. Докажите, что последовательность  $mx_n$  также р.р.  $(\text{mod } 1)$ . Верно ли, что если  $m$  — не целое, то это не верно?

#### Вопросы на хор.

35. Линейная выразимость НОДа (б/д). Доказательство леммы Евклида при помощи алгоритма Евклида.
36. Доказательство леммы Евклида через «идеалы».
37. Доказательство единственности в основной теореме арифметики «от противного».
38. Системы вычетов. Малая теорема Ферма (4 доказательства).

39. Мультипликативность функции Эйлера. Формула с произведением по простым числам: вывод из свойства мультипликативности.
40. Теорема Лагранжа о числе корней многочлена по простому модулю.
41. Распределение простых чисел в натуральном ряде. Функции  $\pi(x)$ ,  $\theta(x)$ ,  $\psi(x)$ . Теорема о равенстве нижних и верхних пределов (формулировка). Асимптотический закон распределения простых (б/д). «Дырки» между соседними простыми числами (б/д).
42. Китайская теорема об остатках.
43. (умение) Решение линейных сравнений и систем линейных сравнений.
44. Сравнения второй степени. Квадратичные вычеты и невычеты. Тождество  $\left(\frac{a}{p}\right) = (-1)^{\sum_{x=1}^{p-1} \left[\frac{2ax}{p}\right]}$ .
45. Сравнения второй степени. Квадратичные вычеты и невычеты. Формула для  $\left(\frac{2}{p}\right)$  (тождеством с суммой по  $\left[\frac{2ax}{p}\right]$  можно пользоваться без доказательства).
46. Матрицы Адамара. Кронекеровское произведение и общая формулировка про  $A \cdot B$ .
47. Матрицы Адамара. Конструкция Пэлли с квадратичными вычетами при  $n = p + 1$ ,  $p = 4m + 3$ .
48. Порядки(показатели) элементов в системах вычетов. Равенство  $\text{ord}(g^l) = \frac{\text{ord } g}{(l, \text{ord } g)}$ . Следствие: если есть порядок  $k$ , то есть порядки и всех делителей  $k$ .
49. Порядки(показатели) элементов в системах вычетов. Если  $\text{ord } g = k$ ,  $\text{ord } h = l$ , и  $(k, l) = 1$ , то  $\text{ord}(gh) = kl$ .
50. Пусть  $\varphi(m) = p_1^{\alpha_1} \cdot \dots \cdot p_s^{\alpha_s}$  — каноническое разложение числа  $\varphi(m)$  на простые сомножители,  $(g, m) = 1$ . В этом случае  $g$  — первообразный корень в  $\mathbb{Z}_m$  тогда и только тогда, когда  $g$  не является решением ни одного из сравнений  $g^{\frac{\varphi(m)}{p_k}} \equiv 1 \pmod{m}$  при  $k = 1, \dots, s$ .
51. (умение) Решение степенных сравнений по простому модулю.
52. Теорема Дирихле о диофантовых приближениях (формулировка и доказательство с использованием принципа Дирихле).
53. Уточнение теоремы Дирихле в случае рациональных дробей.
54. Двумерная теорема Минковского. Ее уточнение для замкнутых множеств (б/д).
55. Применение двумерной теоремы Минковского для передоказательства теоремы Дирихле.
56. Бесконечные цепные дроби. Утверждение о том, что значение бесконечной цепной дроби является иррациональным числом.
57. Бесконечные цепные дроби. Представление иррационального числа в виде бесконечной цепной дроби.
58. Бесконечные цепные дроби. Единственность представления иррационального числа в виде бесконечной цепной дроби.
59. Передоказательство теоремы Дирихле при помощи цепных дробей. Уточнение теоремы Дирихле (б/д). Зависимость качества аппроксимации от скорости роста неполных частных: существование чисел с заданным наперед качеством аппроксимации; золотое сечение как самое плохо приближаемое число (б/д).
60. Алгебраические и трансцендентные числа. Существование трансцендентных чисел (из соображения мощности). Теорема Лиувилля (б/д). Конструкция трансцендентного числа с помощью цепной дроби и теоремы Лиувилля. Сводка результатов о трансцендентности:  $e$ ,  $\pi$ ,  $e + \pi$ ,  $\pi + e^\pi$ ,  $\alpha^\beta$  (теорема Гельфонда), вывод про  $e^\pi$  из теоремы Гельфонда.
61. Решение уравнения Пелля  $a^2 - 2b^2 = \pm 1$ .
62. Решение уравнения Пелля  $a^2 - 3b^2 = \pm 1$ .
63. Равномерно распределенные последовательности  $(\text{mod } 1)$ : три эквивалентные формулировки.
64. Является ли  $\ln n$  р.р.  $(\text{mod } 1)$  последовательностью?
65. Существует ли  $a > 1$ , при которой последовательность  $a^n$  не р.р.  $(\text{mod } 1)$ ?
66. Теорема Вейерштрасса про приближение непрерывной функции (б/д). Равносильность критерия Вейля и интегрального признака.
67. Суммы Гаусса.

#### Вопросы на отл.

68. Проблема Эрдеша–Гинзбурга–Зива при  $d = 2$  и  $n = p$ : нижняя и верхние оценки (формулировка). Доказательство основной леммы.

- 69.** Сравнения второй степени. Квадратичные вычеты и невычеты. Тождество  $\left(\frac{a}{p}\right) = (-1)^{\sum_{x=1}^{\frac{p-1}{2}} \left[\frac{ax}{p}\right]}$  для нечётного  $a$ . (тождеством с суммой по  $\left[\frac{2ax}{p}\right]$  можно пользоваться без доказательства).
- 70.** Сравнения второй степени. Квадратичные вычеты и невычеты. Квадратичный закон взаимности (тождеством с суммой по  $\left[\frac{ax}{p}\right]$  для нечётного  $a$  можно пользоваться без доказательства).
- 71.** Показатели. Первообразные корни. Существование по модулю 2, 4,  $p$ .
- 72.** Показатели. Первообразные корни. Существование по модулю  $p^\alpha$ ,  $\alpha \geq 2$ : формулировка и доказательство леммы. Существование по модулю  $2p^\alpha$ .
- 73.** Показатели. Первообразные корни. Существование по модулю  $p^\alpha$ ,  $\alpha \geq 2$ : формулировка леммы (б/д) и вывод существования из неё. Существование по модулю  $2p^\alpha$ .
- 74.** Показатели. Первообразные корни. Несуществование по модулю  $2^n$ ,  $n \geq 3$ .
- 75.** Показатели. Первообразные корни. Несуществование по модулям, отличным от  $2^\alpha$ ,  $p^\alpha$ ,  $2p^\alpha$ .
- 76.** Распределение простых чисел в натуральном ряде. Функции  $\pi(x)$ ,  $\theta(x)$ ,  $\psi(x)$ . Теорема о равенстве нижних и верхних пределов.
- 77.** Распределение простых чисел в натуральном ряде. Функции  $\pi(x)$ ,  $\theta(x)$ ,  $\psi(x)$ . Теорема Чебышёва (нижняя оценка — с док-вом, верхняя — формулировка).
- 78.** Распределение простых чисел в натуральном ряде. Функции  $\pi(x)$ ,  $\theta(x)$ ,  $\psi(x)$ . Теорема Чебышёва (верхняя оценка — с док-вом, нижняя — формулировка).
- 79.** Решетки в пространствах. Базис и определитель. Многомерная теорема Минковского (для произвольной решетки).
- 80.** Теорема Минковского–Главки и история ее улучшений. Доказательство теоремы Минковского–Главки для октаэдра: определение октаэдра, решётки  $\Lambda_{\bar{a}}$ , числа  $S_{\bar{a}}$ . Переформулировка условия теоремы в виде неравенства на  $p$  и  $n$ . Сведение теоремы к неравенству  $\frac{1}{(p-1)^n} \sum_{\bar{a}} S_{\bar{a}} < 1$ .
- 81.** Доказательство теоремы Минковского–Главки для октаэдра. Определение октаэдра, решётки  $\Lambda_{\bar{a}}$ , числа  $S_{\bar{a}}$ . Лемма для  $S_{\bar{a}}$  (формулировка и доказательство).
- 82.** Доказательство теоремы Минковского–Главки для октаэдра. Определение октаэдра, решётки  $\Lambda_{\bar{a}}$ , числа  $S_{\bar{a}}$ . Лемма для  $S_{\bar{a}}$  (формулировка). Вывод из леммы неравенства  $\frac{1}{(p-1)^n} \sum_{\bar{a}} S_{\bar{a}} < 1$ .
- 83.** Теорема Лиувилля.
- 84.** Доказательство трансцендентности  $e$ . Тождество Эрмита. Определение многочлена  $f(x)$ . Следствие из тождества Эрмита с использованием  $a_k$  (коэффициентов многочлена в предположении алгебраичности числа  $e$ ).
- 85.** Доказательство трансцендентности  $e$ . Тождество Эрмита (б/д). Вид многочлена  $f(x)$ , определение  $F(x)$ , свойства значений  $F(k)$ ,  $f(k)$ ,  $f^{(l)}(k)$  при  $k = 1, \dots, m$ ,  $l = 0, 1, \dots, n-1$ .
- 86.** Доказательство трансцендентности  $e$ . Следствие из тождества Эрмита с использованием  $a_k$  (коэффициентов многочлена в предположении алгебраичности числа  $e$ ) (б/д). Свойства многочлена  $f(x)$  (б/д). Выбор степени  $n$ , оценка левой и правой частей, приведение к противоречию алгебраичности числа  $e$ .