Вопросы к экзамену по дисциплине "Дискретная математика"

1. Множества и классы. Антиномии (парадоксы). Антиномия всемогущества, парадокс «деревенский парикмахер». Антиномия Рассела. Пустое множество. Универсум. Мощность (кардинальное число, порядок) множества. Булеан.

2. Бесконечные множества. Раномощные бесконечные множества, теорема Кантора-Бернштейна. Счетные, несчетные множества. Континуум гипотеза.

3. Отношение. Кортеж. Бинарное отношение. Отношение принадлежности. Отношение включения. Подмножество, надмножество, собственное подмножество. Операции над множествами: объединение (дизъюнкция, сумма), пересечение (конъюнкция, произведение), разность, симметрическая разность, дополнение.

4. Рефлексивное, симметричное, антисимметричное, транзитивное отношения. Отношение предпорядка, порядка, толерантности, эквивалентности.

5. Элементы комбинаторики – сочетания, размещения, перестановки без повторения, с повторениями. Метод включений и исключений. Метод математической индукции.

6. Решение однородных и неоднородных линейных рекуррентных соотношений.

7. Производящие функции и их использование в задачах комбинаторики, решении рекуррентных соотношений.

8. Элементы теории чисел: целые числа, понятия частного, делителя, остатка, доказательство единственности остатка.

9. Элементы теории чисел: наибольший общий делитель (НОД), алгоритм нахождения НОД, взаимнопростые числа, наименьшее общее кратное. Понятие простого числа, доказательство бесконечности простых чисел. Основная теорема арифметики.

10. Теория сравнений: определение, основные теоремы.

11. Малая теорема Ферма и ее доказательство. Функция Эйлера, ее свойства. Обобщение малой теоремы Ферма - теорема Эйлера-Ферма.

12. Методы решения сравнений $ax \equiv b$, основные теоремы о нахождении корней сравнения первого порядка.

13. Алгоритм шифрования без передачи ключей.

14. Алгоритм шифрования RSA.

15. Инволюция (обращение), дополнение, произведение (композиция) отношений. Способы задания отношений. Декартово произведение множеств. Отображение (соответствие). Пустое отображение, полное отображение. Область определения, прообраз (Dom) отображения. Область значений, образ (Im) отображения. Всюду определенные и сюръективные отображения. Образ (im) и прообраз (coim) элемента. Отображение как частично определенная многозначная функция.

16. Бинарная операция и ее основное множество. Алгебра, сигнатура алгебры, тип алгебры. Модель. Способы задания бинарной операции. Таблица Кэли. Группоид. Полугруппа. Моноид. Группа. Абелева группа. Группа симметрий фигуры. Симметрическая группа (группа подстановок). Подгруппа данной группы. Порядок группы. Теорема Лагранжа.