1. Группа, кольцо, поле. Примеры групп, колец, полей. Кольцо вычетов по модулю. Простейшие свойства.
2. Алгоритм Евклида, доказательство, время работы. Реализация с использованием деления на два.
3. Поиск обратного элемента. Китайская теорема об остатках. Восстановление остатка по КТО.
4. Решение линейных сравнений по модулю.
5. Дискретный логарифм и первообразный корень. Функция Эйлера и ее свойства.
6. Теоремы Ферма, Эйлера, Вильсона. Решето Эратосфена за $O(n)$.
7. Дискретное логарифмирование.
8. Использование дискретного логарифмирования для решения нелинейных сравнений.
9. Быстрый алгоритм извлечения квадратных корней по модулю и его обоснование.
10. Проверка чисел на простоту. Наивный алгоритм. Числа Кармайкла, их свойства. Функция $\lambda(n)$.
11. Тест Миллера-Рабина и его обоснование.
12. ρ-эвристика для разложения числа на простые. Эллиптические кривые, группа сложения точек на эллиптической кривой. Применение для разложения числа на простые множители.
13. Аксиомы векторного пространства и их простейшие следствия.
14. Линейная зависимость. Теорема о линейной зависимости. Базис, равносильность определений базиса.
15. Единственность записи вектора в базисе. Изменение координат вектора при переходе от одного базиса к другому.
16. Подпространства, их сумма и пересечение. Теорема о связи размерностей суммы и пересечения.
17. Скалярное произведение и его свойства. Ортогонализация Грама-Шмидта.
18. Прямая сумма подпространств. Ортогональное дополнение. Решение задачи о пересечении сфер.
19. Алгоритм обращения матрицы. Решение задачи «CRC». Матрицы элементарных преобразований.
20. Аффинное пространство, его определение и свойства. Аффинное отображение, дифференциал отображения. Размерность аффинного пространства, аффинные подпространства.
21. Барицентрические комбинации. Аффинная оболочка. Теорема о связи двух определений аффинной оболочки.
22. Гамильтонов цикл. Теорема Редеи-Камиона о гамильтоновости турнира.
23. Теорема Хватала. Теоремы Оре и Дирака как следствие теоремы Хватала.
24. Задача линейного программирования, определение, примеры.
25. Решение задач линейного программирования на плоскости. Метод полуплоскостей.
26. Каноническая форма задач линейного программирования. Переход в каноническую форму. Базисная форма.
27. Алгоритм симплекс-метода, поиск оптимального плана, начиная с некоторого допустимого базисного плана. Корректность алгоритма (допустимость построенных планов, обработка случая неограниченной формы). Время работы.
28. Двойственность в задачах линейного программирования. Правила построения двойственной задачи. Примеры. Теорема о слабой двойственности.
29. Теорема о двойственности задач линейного программирования. Поиск решения двойственной задачи.
30. Поиск допустимого плана. Основная теорема линейного программирования.
31. Паросочетания в графах. Теорема о построении максимального паросочетания и минимального контролирующего множества. Способ их одновременного построения, свойства.
32. Алгоритм Хопкрофта-Карпа. Обоснование.

33. Алгоритм Хопкрофта-Карпа. Время работы.

34. Венгерский метод решения задачи о назначениях. Наивный метод и проблемы, с ним связанные.

35. Венгерский метод решения задачи о назначениях за $O(n^3)$.

36. Алгоритм Укконена.

37. Свойства правых контекстов и суффиксной эквивалентности.

38. Изменение правого контекста при добавлении символа. Основная теорема о раздвоении состояния. Идея алгоритма построения суффиксного автомата.