МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ им. М.В.ЛОМОНОСОВА

Факультет Вычислительной математики и кибернетики

Вопросы к экзамену по курсу «Прикладная алгебра»

(5 семестр, III поток, 2018/19 уч. год)

1. Конечное поле и его характеристика. Мультипликативная группа, примитивный элемент поля Галуа и его нахождение. Основная теорема алгебры.
2. Алгоритм Евклида и его применение.
3. Соотношение Безу и расширенный алгоритм Евклида.
4. Неприводимые многочлены: их существование и нахождение в конечных полях.
5. Построение конечных полей с помощью неприводимых многочленов (привести пример). Изоморфизм конечных полей.
6. Векторное пространство многочленов. Базис в $\mathbb{F}_p^n$. Поля Галуа как векторные пространства. Подполя конечного поля.
7. Минимальные многочлены над конечным полем: примеры и свойства. Корнями какого многочлена являются все элементы конечного поля? Делителями какого многочлена являются все неприводимые многочлены n-й степени?
8. Теорема о степени любого неприводимого делителя бинома $x^{p^n-1}-1$.
9. Теорема о корнях неприводимого многочлена. Многочлены над конечным полем: решение уравнений.
10. Алгоритм нахождения всех корней многочлена $f(x)$ над полем $\mathbb{F}_p$.
11. Мультипликативная группа расширения поля. Существование неприводимого многочлена степени n над полем $\mathbb{F}_p$.
12. Лемма о числе неприводимых нормированных многочленов из $\mathbb{F}_p^n$. Среднее число неприводимых многочленов.
13. Изоморфизм полей Галуа с одинаковым числом элементов.
14. Теорема о неприводимом нормированном многочлене-делителе порождающего элемента идеала.
15. Циклическое пространство: определение и примеры.
16. Количество и степени неприводимых делителей бинома x^n-1.
17. Задачи построения кодов, исправляющих ошибки. Основные понятия метрики на единичном кубе.
18. Групповые (линейные) коды: определения, свойства. Кодовое расстояние. Построение кода как задача плотной упаковки.

19. Линейные коды. Порождающая и проверочная матрица. Систематическое кодирование и синдромное декодирование. Примеры.
20. Теорема Хэмминга. Пример построения кода Хэмминга.
21. Коды Хэмминга как частный случай кодов БЧХ. Алгоритм декодирования. Примеры.
22. Циклические коды. Порождающий полином. Систематическое кодирование и синдромное декодирование. Примеры.
23. Коды БЧХ как частный случай циклических кодов. Идея построения кода БЧХ и оценка его кодового расстояния.
24. Декодирование БЧХ кодов. Синдромный полином и полином локаторов ошибок. Ключевое уравнение. Декодер Евклида. Примеры.
25. Основные понятия криптографии. Правило стойкости О. Керкгоффса. Симметрические и асимметрические шифрсистемы. Алгоритм быстрого возведения в степень. Задача о рюкзаке.
26. Односторонняя функция. Односторонняя функция с секретом. Электронная цифровая подпись. Пример использования односторонней функции с секретом при решении задачи о рюкзаке.
27. Протокол Диффи-Хеллмана выработки общего секретного ключа по открытому каналу связи.
28. Система шифрования RSA.
29. Алгоритм проверки непростоты числа на основе малой теоремы Ферма.
30. ρ-алгоритм Полларда сплиттинга чисел.
31. *(p-1)*-алгоритм Полларда факторизации чисел.
32. Дискретное логарифмирование. Криптосистема Эль-Гамаля.
33. Алгоритм согласования для нахождения дискретного логарифма.