МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ им. М.В.ЛОМОНОСОВА

Факультет Вычислительной математики и кибернетики

Вопросы к экзамену по курсу «Прикладная алгебра»

5 семестр, III поток, 2019/20 уч. год

1. Конечное поле и его характеристика. Мультипликативная группа, примитивный элемент поля Галуа и его нахождение.
2. Алгоритм Евклида.
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?
8. Теорема о степени любого неприводимого делителя бинома $x^{p^n-1}-1$.
9. Алгоритм нахождения всех корней многочлена *f(x)* над полем $\mathbb{F}_p$.
10. Мультипликативная группа поля. Существование неприводимого многочлена степени *n* над полем $\mathbb{F}_p$.
11. Лемма о числе неприводимых нормированных многочленов из $\mathbb{F}_p^n$.
12. Изоморфизм полей Галуа с одинаковым числом элементов.
13. Теорема о неприводимом нормированном многочлене-делителе порождающего элемента идеала.
14. Циклическое пространство: определение и примеры.
15. Количество и степени неприводимых делителей бинома x^n-1.
16. Задачи построения кодов, исправляющих ошибки. Задача плотной упаковки и экстремальные коды.
17. Линейные коды: определения, свойства, характеристики.
18. Линейные коды: порождающая и проверочная матрица. Систематическое кодирование. Декодирование по максимуму правдоподобия.
19. Теорема Хэмминга. Пример построения кода Хэмминга.
20. Коды Хэмминга как частный случай кодов БЧХ. Алгоритм декодирования. Примеры.

21. Циклические коды. Порождающий полином. Систематическое кодирование. Синдромное декодирование.
22. Коды БЧХ как частный случай циклических кодов. Идея построения кода БЧХ и оценка его кодового расстояния.
23. Декодирование БЧХ кодов. Синдромный полином и полином локаторов ошибок. Ключевое уравнение. Декодер Евклида.
24. Основные понятия криптографии. Правило стойкости О. Керкгоффса. Симметрические и асимметрические шифрсистемы. Алгоритм быстрого возведения в степень. Задача о рюкзаке.
25. Односторонняя функция. Односторонняя функция с секретом. Электронная цифровая подпись. Пример использования односторонней функции с секретом при решении задачи о рюкзаке.
26. Протокол Диффи-Хеллмана выработки общего секретного ключа по открытому каналу связи.
27. Система шифрования RSA.
28. Алгоритм проверки непростоты числа на основе малой теоремы Ферма.
29. ρ-алгоритм Полларда сплиттинга чисел.
30. Дискретное логарифмирование. Криптосистема Эль-Гамаля.
31. Алгоритм согласования для нахождения дискретного логарифма.
32. Уравнения ЭК в конечных полях различных характеристик. Геометрическая интерпретация сложения и удвоения точек ЭК.
33. Задача ECDLP нахождения дискретного логарифма в группе точек ЭК.
34. «Перевод» обычного криптоалгоритма в эллиптический.