МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ им. М.В.ЛОМОНОСОВА

Факультет Вычислительной математики и кибернетики

Вопросы к экзамену по курсу «Прикладная алгебра»

группы 320, 321, 323, 327, 328 (III поток), 2020/21 уч. год

1. Конечное поле и его характеристика. Мультипликативная группа, примитивные элементы и их нахождение.
2. Алгоритм Евклида.
3. Соотношение Безу и расширенный алгоритм Евклида.
4. Неприводимые многочлены. Существование неприводимых многочленов с коэффициентами из конечных полей.
5. Построение конечных полей с помощью неприводимых многочленов (привести пример). Изоморфизм конечных полей.
6. Векторное пространство многочленов. Базис в 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 F_p.
10. Мультипликативная группа поля. Существование неприводимого многочлена степени n над полем F_p.
11. Лемма о числе неприводимых нормированных многочленов из F_p^n.
12. Теорема о неприводимом нормированном многочлене-делителе порождающего элемента идеала.
13. Циклическое пространство: определение и примеры.
14. Количество и степени неприводимых делителей бинома x^n-1.
15. Задачи построения кодов, исправляющих ошибки. Задача плотной упаковки и экстремальные коды.
16. Линейные коды: определения, свойства, характеристики.
17. Линейные коды: порождающая и проверочная матрица. Систематическое кодирование. Декодирование по максимуму правдоподобия.
18. Циклические коды. Порождающий полином. Неистематическое и систематическое кодирование. Синдромное декодирование.

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