МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ им. М.В.ЛОМОНОСОВА

Факультет Вычислительной математики и кибернетики

Теоретический минимум к экзамену по курсу «Прикладная алгебра»

группы 320, 321, 323, 327, 328 (III поток), 2020/2021 уч. год

Незнание ответа на ***любой*** из нижеследующих вопросов
(для каждого понятия может потребоваться привести пример)
автоматически влечет неудовлетворительную оценку за экзамен. При этом знание ответов только на данные вопросы не обеспечивает ещё положительной оценки.

1. Группы. Подгруппы и факторгруппы. Теорема Лагранжа.
2. Циклические группы. Бесконечная и конечная циклические группы, количество порождающих элементов в них.
3. Кольца. Подкольца, идеалы, главные и максимальные идеалы.
4. Кольца. Классы вычетов и факторкольца. Целостные и евклидовы кольца.
5. Поля: определение, характеристика поля, конечные и бесконечные поля. Для каких q существуют поля из q элементов? Построение расширений простых конечных полей.
6. Нахождение всех корней неприводимого многочлена в поле его расширения. Найти все корни многочлена $f(x)=x^4+x+1 \in F_2[x]$.
7. Минимальный многочлен элемента конечного поля, алгоритм его нахождения.
8. Построение кода Хэмминга.
9. Линейные коды и их свойства. Порождающая и проверочная матрицы линейного кода.
10. Циклические коды. Определение, построение, кодирование циклическими кодами.
11. Определение кодов БЧХ. Пример кода длины $n=15$, с исправлением двух ошибок.
12. Односторонняя функция и односторонняя функция с секретом. Электронная цифровая подпись.
13. Протокол Диффи-Хеллмана выработки общего секретного ключа по открытому каналу связи.
14. Алгоритм проверки простоты числа на основе малой теоремы Ферма.
15. Эллиптические кривые (ЭК) в короткой форме Вейерштрасса ЭК как группа. Порядок группы точек и порядок точки ЭК. Теорема Хассе.