МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ им. М. В. ЛОМОНОСОВА

Факультет Вычислительной математики и кибернетики

Теоретический минимум к экзамену по курсу «Прикладная алгебра»

5 семестр, III поток, 2019/2020 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 них не обеспечивает положительной оценки.

1. Группа. Подгруппы, факторгруппы, индекс группы по подгруппе. Теорема Лагранжа. Примеры.
2. Циклические группы. Примеры. Бесконечная и конечная циклическая группа, количество порождающих элементов в них.
3. Кольцо. Подкольца, факторкольца, идеалы, главные идеалы. Евклидовы кольца. Примеры.
4. Обобщённый алгоритм Евклида.
5. Поле: характеристика, примеры. Для каких q существуют поля *GF(q)*? Построение расширений простых конечных полей.
6. Нахождение всех корней неприводимого многочлена в поле его расширения. Найти все корни многочлена $f(x) = x^4 + x + 1 \in \mathbb{F}_2[x]$.
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. Определение кодов БЧХ. Пример кода с исправлением двух ошибок.
11. Декодирование кода БЧХ.
12. Основные понятия криптографии. Правило стойкости О. Керкгоффса. Симметрические и асимметрические шифрсистемы.
13. Односторонняя функция и односторонняя функция с секретом. Электронная цифровая подпись.
14. Протокол Диффи-Хеллмана выработки общего секретного ключа по открытому каналу связи.
15. Алгоритм проверки простоты числа на основе малой теоремы Ферма.
16. Эллиптические кривые (ЭК) в короткой форме Вейерштрасса. ЭК как группа. Порядок группу точек и порядок точки ЭК. Теорема Хассе.