МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ им. М.В.ЛОМОНОСОВА

Факультет Вычислительной математики и кибернетики

Теоретический минимум к экзамену по курсу «Прикладная алгебра»

(5 семестр, III поток)

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, фактор-группы, индекс группы по подгруппе. Теорема Лагранжа.
2. Циклическая группа. Количество порождающих элементов. Подгруппы циклической группы.
3. Кольцо. Подкольца, фактор-кольца, идеалы, главные идеалы. Евклидовы кольца.
4. Расширенный алгоритм Евклида и его применение.
5. Поля. Построение конечных полей с помощью неприводимых многочленов. Полиномиальное и степенное представление элементов поля.
6. Алгоритм нахождения всех корней многочлена над простым конечным полем.
7. Минимальный многочлен элемента конечного поля, алгоритм его нахождения.
8. Построение кода Хэмминга.
9. Построение кода БЧХ.
10. Схема декодирования кода БЧХ.
11. Основные понятия криптографии. Правило стойкости О. Керкгоффса. Симметрические и асимметрические шифрсистемы.
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 непростоты числа на основе малой теоремы Ферма.