Экзаменационная программа по курсу «Математические основы защиты информации», направление подготовки «ФИИТ», 3 курс, 1 семестр 2017–2018 учебного года

Алгебраические системы с двумя операциями

Теория колец. Идеалы, определение, примеры, нулевой, единичный, собственные и несобственные. Главный идеал, кольцо главных идеалов. Идеал, порожденный несколькими элементами, нетерово кольцо. Необходимые и достаточные условия соотношений $(a) = \{0\}$, $(a) = R$, $\{0\} \subsetneqq (a) \subsetneqq R$, следствия. Идеалы в кольцах $\mathbb{Z}$ и $F[x]$. Теорема Гильберта о базисе (б/д). Гомоморфизм колец. Ядро и образ гомоморфизма, критерии инъективности и сюръективности гомоморфизма. Факторкольцо. Канонический гомоморфизм. Теорема о гомоморфизмах в случае колец. Максимальный идеал. Теорема о расширении произвольного идеала до максимального (б/д). Критерии максимальности идеалов в случае колец $\mathbb{Z}$ и $F[x]$. Теорема о факторкольце по максимальному идеалу. Структура факторкольца в случае кольца полиномов, критерий обратимости смежного класса.

Отношение делимости в кольце. Критерий существования единичного элемента. Ассоциированные элементы, теорема о свойствах, равносильных ассоциированности. Приводимые и неприводимые элементы, свойства неприводимых элементов. Евклидовы кольца, примеры евклидовых колец. Существование единичного элемента в евклидовом кольце. Критерий обратимости элемента евклидова кольца. Идеалы евклидова кольца. Ассоциированность элементов с равными евклидовыми нормами. Неприводимость элемента с евклидовой нормой θ_1. Наибольший общий делитель в евклидовом кольце, свойства неприводимых элементов в евклидовом кольце. Фундаментальная теорема о разложении на неприводимые множители в евклидовом кольце.

Теория полей. Характеристика поля. Свойства характеристики. Изоморфизм полей. Подполе, критерий того, что подмножество является подполем. Расширения полей. Конечные расширения полей, степень расширения. Теорема о степенях, следствия. Простые поля, теорема существования простого подполя. Теорема о подполях, изоморфных простому подполю. Поля Галуа. Характеристика и число элементов произвольного конечного поля, следствие о числе элементов конечного поля. Алгебраические элементы, алгебраическое расширение. Минимальный и аннулирующий многочлен алгебраического элемента. Свойства аннулирующих многочленов. Теорема о расширении $K(\alpha)$ для алгебраического элемента α. Теорема существования расширения, в котором неприводимый многочлен имеет корень. Следствие о существовании расширения, в котором многочлен разлагается на линейные множители. Теорема о корнях многочлена $x^{p^n} - x$ над полем характеристики p, следствие о существовании поля с p^n элементами. Поле частных.

Теория чисел

Квадратичные вычеты. Дискретное логарифмирование в конечной циклической группе. Двучленные уравнения. Вычеты и невычеты степени n. Квадратичные вычеты по простому нечетному модулю. Число решений сравнений второй степени.

Критерий Эйлера. Символ Лежандра. Свойства символа Лежандра. Символ Якоби. Свойства символа Якоби. Сравнения по модулю p^k. Сравнения по модулю 2^k (б/д).

Цикличность группы $\mathbb{Z}_n^*$. Лемма о четности функции Эйлера. Достаточные условия нецикличности группы $\mathbb{Z}_n^*$, следствия. Окончательный результат о цикличности группы $\mathbb{Z}_n^*$ (б/д). Структура группы $\mathbb{Z}_{2^n}^*$ (теорема о числах 5^{2^n}, следствие об элементе 5 в группе $\mathbb{Z}_{2^n}^*$, теорема об изоморфизме для группы $\mathbb{Z}_{2^n}^*$.)

Введение в теорию информации и криптографию

Определение энтропии. Две леммы. Неравенства для энтропии. Совместная энтропия, теорема о совместной энтропии. Условная энтропия ($H(X|Y=y)$ и $H(X|Y)$, свойства этих характеристик). Понятие о дискретном стационарном источнике, теорема о характеристиках дискретного стационарного источника (б/д). Неравномерное побуквенное кодирование. Однозначно декодируемые и префиксные коды. Неравенство Крафта. Теорема Макмиллана (б/д). Прямая и обратная теоремы побуквенного кодирования. Код Шеннона, префиксность кода Шеннона. Код Хаффмена. Определение криптосистемы, примеры криптосистем. Криптосистема RSA.