Содержание лекций по алгебре в первом модуле

1.Свойства делимости в кольце целых чисел. Теорема о делении с остатком. Идеалы — определение, идеалы порожденные набором элементов,в целых числах все идеалы главные. НОД и его единственность, теорема о его линейном представлении. Критерий разрешимости линейного диофантова уравнения. Алгоритм Евклида.

2. Взаимная простота (2 определения), лемма об отбрасывании взаимно простого множителя, простые числа и их основное свойство. Основная теорема арифметики (существование и единственность). "Контрпримеры" к ОТА. Степень вхождения и её свойства. Делимость, свойство “быть степенью” в терминах канонического разложения,НОД и НОК. Формулы для количества и суммы делителей. Понятие группы, примеры абелевых групп.

3. Отношения, отображения, Инъекция- сюръекция-биекция. Основной пример группы: симметрическая группа. Кольцо, поле и близкие понятия. Сравнимость по модулю сравнимость — отношение эквивалентности, согласованность с кольцевыми операциями, построение кольца вычетов. Редукция по простому модулю, пример. Обратимые элементы в кольцах вычетов, когда кольцо вычетов -- поле. Деление в кольцах вычетов примеры.

4. Сокращение в группах и кольцах, кольца без делителей нуля. Решение Линейного диофантова уравнения. Мультипликативная группа кольца. Порядок элемента, его свойства. Теорема Лагранжа. Малая теорема Ферма. Циклическая группа, критерий цикличности. Подгруппа, подкольцо и т.п. Гомоморфизмы групп и колец.

5. Изоморфизм групп, примеры. Конечная циклическая группа изоморфна группе вычетов. Группы простых порядков. Прямое произведение групп и колец (и полей). Китайская теорема об остатках (кольцевая версия). Переформулировка в терминах систем сравнений, алгоритм решения системы. Порядок мультипликативной группы: функция Эйлера, явная формула,

6. Мультипликативность функции Эйлера, другие мультипликативные функции. Теорема Эйлера, её улучшаемость. Теорема о цикличности мультипликативных групп кольца вычетов, часть доказательства (сведения к случаю степени простого). Первообразный корень по модулю p^2. Биективность возведения в степень в кольце вычетов. Алгоритм RSA.

7.Бесконечность простых и их частота. Теорема Люка и тест Люка как хороший вероятностный тест. Взламываемость простых чисел, полученных методом Люка. Тест Ферма, абсолютно псевдопростые числа. Тест Рабина Миллера и почему он вероятностно отсекает составные числа. Первообразный корень по модулю p^k.