Программа по курсу «эллиптические кривые и криптография». Осенний семестр 2015.

1) Понятие группы, подгруппы, абелевой группы. Теорема о строении конечно-порождённой абелевой группы (формулировка). Когда прямая сумма двух циклических групп — циклическая группа. Смежные классы. Теорема Лагранжа. Нормальная подгруппа. Факторгруппа.
2) Понятие кольца, поля. Идеалы. Факторкольца. Факторкольца по простым и максимальным идеалам. Максимальные идеалы в кольце многочленов от 1 переменной над полем. Теорема о строении конечных полей (формулировка).
3) Алгебраические и трансцендентные расширения полей. Конечные расширения. Базис трансцендентности. Корректность определения степени трансцендентности. Доказательство того, что алгебраические элементы образуют поле.
4) Теорема Гильберта о базисе идеала.
5) Аффинное алгебраическое многообразие. Алгебра регулярных функций. Морфизмы аффинных алгебраических многообразий. Связь с гомоморфизмами алгебр регулярных функций.
6) Топология Зарисского.
7) Поле рациональных функций неприводимого аффинного многообразия. Просективные многообразия. Покрытие аффинными картами.
8) Теорема Безу.
9) Касательное пространство. Инвариантное определение касательного пространства.
10) Особые точки и точки перегиба плоской кривой. Гессиан. Определение эллиптической кривой.
11) Нормальная форма Вейерштрасса.
12) Дискриминант и j-инвариант эллиптической кривой. Эквивалентность кривых с одинаковым j-инвариантом.
13) Точки перегиба эллиптических кривых. Инволюции. Подгруппа в группе автоморфизмов, порождённая инволюциями.
14) Групповой закон на эллиптической кривой. Доказательство ассоциативности для общих точек.
15) Явные формулы для группового закона.
16) Нерациональность эллиптических кривых.
17) Решётки на плоскости. Эллиптические функции. Порождающие поля эллиптических функций.
18) Дифференциальное уравнение для функции Вейерштрасса.
19) Изоморфизм полей рациональных функций на эллиптической кривой и эллиптических функций. Эквивалентность решёток. Модулярная группа.