ЭЛЛИПТИЧЕСКИЕ КРИВЫЕ И ИХ АРИФМЕТИЧЕСКИЕ СВОЙСТВА

д.ф.-м.н. Д.В. Осипов

Краткая аннотация:

Эллиптическая кривая над полем – это гладкая проективная кривая рода 1, т.е. обладающая не имеющей полюсов и нулей рациональной дифференциальной 1-формой, или эквивалентно: гладкая кубическая кривая в двумерном проективном пространстве, имеющая точку, определенную над основным полем. На множестве точек эллиптической кривой, определенных над основным полем, можно ввести структуру абелевой группы. Если основное поле – это поле комплексных чисел, то данная группа не слишком интересна, так как изоморфна двумерному тору. Если основное поле – конечное поле, то получаем конечную группу, имеющую множество применений в теории кодирования. В случае, если основное поле – это поле рациональных чисел, то можно доказать, что получившаяся абелева группа конечно порождена. С инвариантами этой группы связано множество знаменитых гипотез в арифметической алгебраической геометрии. От слушателей курса потребуется знание основ теории Галуа, теории *p*-адических чисел и начальные знания по теории алгебраических кривых.

Предварительная программа:

- Кривые рода 0 над алгебраически незамкнутыми полями. Принцип Хассе и его справедливость для кривых рода 0 над полем **Q**.

- Кубические кривые, кривые рода 1, Вейерштрассова нормальная форма.

- Когомологии Галуа, формы алгебраических кривых, главные однородные пространства.

- Нарушение принципа Хассе для кривых рода 1 над полем **Q.** Группа Шафаревича–Тейта.

- Группа Зельмера и ее конечность.

- Высота точки эллиптической кривой над полем **Q.** Каноническая высота Тейта. Теорема Морделла–Вейля.

- Кольцо эндоморфизмов эллиптической кривой. Эллиптические кривые над конечными полями. Теорема Хассе об оценке числа точек эллиптической кривой над конечным полем.

- Эллиптические кривые над *p*-адическими полями. Редукция эллиптической кривой. Вырожденные эллиптические кривые и их связь с аддитивной и мультипликативной группой поля.

- Точки кручения на эллиптической кривой над полем **Q.** Теорема Нагеля–Лютц.

- Дзета-функция алгебраической кривой над конечным полем. L-функция эллиптической кривой над полем **Q**. Гипотезы Берча и Суиннертона-Дайера.

- Условный алгоритм Манина отыскания базиса группы рациональных точек и порядка группы Шафаревича–Тейта для эллиптической кривой над полем **Q**.