

# Seminar: Elliptic Curves

February 3, 2009

In this seminar, we will study the basic theory of Elliptic Curves. We shall begin with a geometric study of plane curves. Then we will specialize to the study of a specific family of plane curves: Elliptic Curves. These curves are characterized by the additional property that their set of rational solutions is in fact an abelian group. The main object of the course will be to study the structure of this group. In particular, the course will culminate in the theorem of Mordell-Weil which states that this group is a finitely generated abelian group. Along the way, we shall study some basic notions of algebraic geometry including the notion of projective space. We shall follow closely the text of Dale Husemoller, "Elliptic Curves".

## List of Talks

**Talk 1:** Sections 1.1 and 1.2. An introduction to the chord-tangent approach to the group law on Elliptic Curves. Some specific examples and illustrations of the group law.

**Talk 2:** Sections 1.3 – 1.4. Explicit study of the families  $y^2 = x^3 + ax$  and  $y^2 = x^3 + a$ . Section 1.4 computes the image of multiplication by 2 on the elliptic curve; this in turn will be crucial later for the proof of the Mordell-Weil theorem.

**Talk 3:** Appendix to Chapter 2 (all sections). Cover the basic theory of divisibility properties of factorial rings and apply it to polynomial rings. Develop the basic background for algebraic curves (recall valuations).

**Talk 4:** Sections 2.1 – 2.2. Define projective spaces and discuss irreducible algebraic curves and hypersurfaces.

**Talk 5:** Sections 2.3 – 2.4. Basic intersection theory for curves in projective space. Discuss why projective spaces are the natural setting for intersection

theory of curves.

**Talk 6:** Sections 3.1 – 3.3. Define the group law on a nonsingular cubic. Discuss normal forms. Explain the discriminant and the  $j$ -invariant.

**Talk 7:** Sections 3.4 – 3.6. Isomorphisms classification of curves with same  $j$ -invariant. Section 3.4 deals with characteristic not equal to 2, 3 while sections 3.5 and 3.6 deal with the characteristic 2 and 3 case respectively.

**Talk 8:** Sections 5.1 – 5.3. Discuss the reduction mod  $p$  of projective spaces and algebraic curves. In particular, discuss the case of elliptic curves, their normal forms and good reduction.

**Talk 9:** Sections 5.4.5.5. Show that at a prime of good reduction the reduction map is a group homomorphisms. Describe the kernel of this map in terms of the  $p$ -adic filtration. Prove the Nagell-Lutz theorem.

**Talk 10:** Sections 6.1 – 6.4. The first part of the proof of Mordell-Weil. Discuss Fermat descent and finiteness of  $[E(\mathbb{Q}) : 2E(\mathbb{Q})]$ . Also discuss the case of  $\mathbb{Q}$  replaces by an arbitrary number field  $K$ .

**Talk 11:** Sections 6.5 – 6.7. Develop the theory of heights and finish the proof of Mordell-Weil.

### References:

- 1: Husemoller, Elliptic Curves.
- 2: Silverman, The Arithmetic theory of Elliptic Curves.

### Notes for giving a talk

Each speaker will be required to meet both Gereon and Deepam at least two weeks in advance to discuss the material of their talks. The speaker should be familiar with the material of their talk and come prepared with questions. The speaker will again be required to meet one week in advance of the talk. Here the speaker should come prepared with an outline of their talk.