Algebraic Geometry

Zandi

October 27, 2013

THIS IS A DRAFT. Expect inaccuracte and incomplete information.

Introduction

1 Conic Sections

Use conic sections to illustrate some basics here and provide necessary theorems/tools for elliptic curve section. Will draw heavily from the book

2 Bezout's Theorem

Bezout's theorem will be important later, but we probably won't be able to fully prove it here. However, the book does prove the limited cases that we'll most rely on.

3 Elliptic Curves

One of the more interesting sections. Definitely need to cover proving the given construction on the non-singuler elliptic curve creates a group. Should also cover how in practice for crypto the identity is chosen as the point at infinity, allowing for much cheaper computation.

4 Regular Polyhedra??

If we even get here, this should be a neat topic to talk about for a bit to offset the earlier material.