Honors Project Proposal

Cecylia Bocovich

Faculty Sponsor: David Bressoud

1 Project Description

The title of this project will be Explorations of the Orders of Elliptic Curves and their Applications to Public-Key Cryptography and will involve the study of elliptic curves modulo p and their role in modern cryptography.

An elliptic curve modulo p is a cubic curve, determined by formula $y^2 = x^3 + ax + b$ with coefficients in the field F_p and at least one point (x, y) with coordinates in F_p. The project will start out with the computational explorations of orders of elliptic curves in various fields F_p where p is a prime number. This will be done with mathematical software such as Mathematica. The goal of the project will be to analyze and attempt to discover patterns in the orders of these curves. These patterns may say something about the difficulty of one-way functions involving elliptic curves. Exploring the mathematics behind these patterns and the implications they hold for public key cryptography will be an ongoing part of the project as well.

2 Timeline

May: Initial reading and background knowledge.

June - July: Continued reading and exploration of the problem.

August: Meet and discuss project. Continued background readings and begin computations of orders of these elliptic curves.

Fall Semester: Meet through the fall to compute the orders of elliptic curves and explore the patterns observed in these computations. Explore the possible implications of these patterns in public-key cryptography.

December: First rough draft completed the first week in December.

Spring Semester: Complete research and paper.