

# COMPLEX MULTIPLICATION ON ELLIPTIC CURVES

COLIN LITTLE

ADVISOR: CHRISTOPHER TOWSE

## 1. PROJECT DESCRIPTION

I have recently been exposed to the area of mathematics involving elliptic curves. These curves are extremely useful in many areas of mathematics, including an area that I am very interested in, cryptography. For my thesis I will begin by examining some basic theory of elliptic curves, looking at groups of rational points on elliptic curves, and then moving on to more advanced areas. One area of interest is the idea of complex multiplication of elliptic curves. That is, elliptic curves such that there exists an endomorphism from the curve to itself that is not a multiplication by  $n$  map. These are interesting curves to study, since most curves do not include this property. This will be the major focus of my research, although I hope that while researching into this area I could uncover other interesting theoretical questions that could be addressed in the thesis.

## 2. SUMMER READING AND PREPARATIONS

As I stated earlier, I am very interested in cryptography, and elliptic curves have become very important in this field. Over the summer I will be working for a communications company doing research and writing monographs on various aspects of cryptography and cryptographic protocols. I plan on doing some work on elliptic curve cryptography for this project. So, this will provide me with additional insight into these mathematical objects that will help me gain a wider and more concrete picture of their use. Also, in working with these curves in a cryptographic setting I hope to motivate questions that could be applicable to my thesis.

This summer work will hopefully be continued into next year with a mathematics clinic based around this research into cryptography. So, I will also be working closely with elliptic curves outside of thesis, (albeit in a different context,) next year. This dual exposure will, (I hope,) provide me with an excellent background and also help to really open up the field for interesting topics to discuss in the thesis.

I have also started doing some preliminary reading from Joseph Silverman and John Tate's text, "Rational Points on Elliptic Curves," which provides good background material.