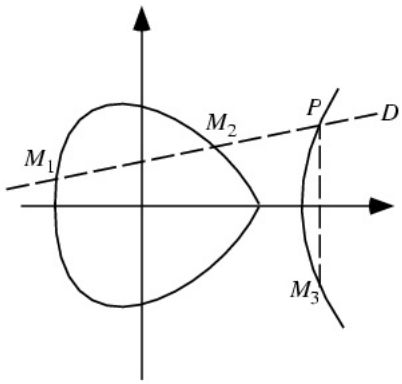
AN INVESTIGATION ON THE ALGEBRAIC AND ANALYTIC PROPERTIES OF ELLIPTIC CURVES

URA PROPOSAL, FALL 2006
HAOKUN XU, '08
ADVISED BY NICK ROGERS

We propose to study the properties of a non-singular elliptic curve, which is the locus of points satisfying the equation

$$E : y^2 = f(x), \qquad f(x) = x^3 + ax + b$$

where a, b are integers such that $f(x)$ has distinct roots, so that the curve has no cusps nor self intersections. The project will begin with the study of the set of rational points (points with rational coordinates) on an elliptic curve, denoted $E(\mathbb{Q})$. Define the "addition" of two points M_1 and M_2 to be the point M_3 on the elliptic curve whose reflection across the x-axis is collinear with M_1 and M_2 (see figure below[1]).



This definition of addition can be shown to be commutative and associative. Furthermore, define the "identity" as $\mathcal{O}$, the point at infinity, and the "inverse" of a point to be its reflection across the x-axis. With these definitions, $E(\mathbb{Q})$ under our addition law is an abelian group. The Mordell-Weil Theorem states that $E(\mathbb{Q})$ is finitely generated, so the group of rational points on an elliptic curve is of the form

$$E(\mathbb{Q}) = E_{tors}(\mathbb{Q}) \oplus \mathbb{Z}^r,$$

where $E_{tors}(\mathbb{Q})$ is the torsion subgroup of points with finite order and r is called the rank of the elliptic curve. The Nagell-Lutz Theorem and Mazur's Theorem give a good characterization of the torsion subgroup, but the rank is less well-understood. We can use Selmer's descent technique to reduce the problem of finding the rank of an elliptic curve to determining the solvability of certain quartic diophantine equations. We will use these techniques to give an upper bound on the rank of certain elliptic curves and to help us study questions such as

[1] http://mathworld.wolfram.com/EllipticCurve.html

(1) For a given elliptic curve E, how can one compute the structure of the torsion subgroup and the rank of that curve?
(2) When is r non-zero?
(3) What is parity of r?
(4) How can we construct elliptic curves of a certain, fixed, rank?
(5) What types of groups can occur (e.g., if $E_{tors}(\mathbb{Q}) \cong \mathbb{Z}/3\mathbb{Z}$, what values can r take on)?

It is also possible to study the rank by computing the so-called analytic rank (which is equal to the rank if a conjecture by Birch and Swinnerton-Dyer is correct). Assuming the BSD conjecture, complex analytic methods can shed light on some of the above questions, especially (2) and (3).

We will then continue our project by taking a fixed elliptic curve (e.g., $E : y^2 = x^3 + x$) and considering the quadratic twist of this elliptic curve,

$$E^d : dy^2 = x^3 + x,$$

where d is a square free integer, and ask similar questions regarding its group structure. Furthermore, we will consider questions such as

(1) Is there a bound on the rank of E^d when d is prime?
(2) What can we say about the rank of E^d when d is of a certain residue class?
(3) What is the average rank of E^d as d varies?

Other possible subjects of study include the group of points of an elliptic curve over other fields, such as the complex numbers, $\mathbb{C}$ or a finite field $\mathbb{F}_q$. Fairly recent developments in the theory of elliptic curves gives applications to public-key cryptography and Lenstra's Elliptic Curve Method for factoring integers, which we might also study.

For the first part of the project, we will reference "Rational Points on Elliptic Curves" by Joseph Silverman and John Tate. Later, we will move on to "Introduction to Elliptic Curves and Modular Forms" by Neal Koblitz and "Elliptic Curves" by Dale Husemöller.