DETERMINING THE RANK OF ELLIPTIC CURVES WITH LOCAL DATA

CORINNE SHERIDAN

1. Introduction

My research lies in algebraic number theory, a branch of mathematics which studies prime numbers in the context of algebraic field extensions. In particular, I study properties of elliptic curves in the context of the Birch and Swinnerton-Dyer (BSD) conjecture, connecting the rank of the elliptic curve with the number of solutions modulo prime numbers p. The BSD conjecture connects the order of the L-function, $L(E, s)$ of the elliptic curve E at $s = 1$ with the rank of the elliptic curve. Elliptic curves have applications in cryptography and offer a powerful tool for proofs in number theory.

1.1. **Background.** An algebraic number is a root of a polynomial $a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$, where the coefficients $\{a_i\}$ are rational numbers, i.e. numbers that can be written as a fraction of integers. An algebraic integer is an algebraic number where $a_n = 1$ and all other a_i are integers. Algebraic number theory considers number fields, finite extensions of the rational numbers $\mathbb{Q}$, and the prime ideals of the ring of integers, the ring of all algebraic integers over that number field.

One major focus of algebraic number theory is the study of elliptic curves, curves which can be written in the form:

$$E : y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6.$$

Elliptic curves can be defined over a general number field $K/\mathbb{Q}$, and extensive information can be found by looking at the elliptic curve in the context of different prime ideals $\mathfrak{p}$. My research focuses on elliptic curves defined over $\mathbb{Q}$ and the number of solutions of the curve modulo primes p.

2. Current Research

For an elliptic curve E over $\mathbb{Q}$, let N_p denote the number of points the curve E when it is reduced modulo p, i.e. the number of points on E over $\mathbb{F}_p$, the finite field with p elements. Then, for primes not dividing the discriminant Δ of E, define

$$a_p = p + 1 - N_p.$$

Further, the Mordell-Weil Theorem states that the number of rational points of an elliptic curve is finitely generated, and the group has the structure $\mathbb{Z}^r \times E_{tors}(\mathbb{Q})$ where the torsion subgroup is finite, and r is the algebraic rank of the curve. The L-function for the elliptic curve is defined to be:

$$L(E,s) = \prod_{p|\Delta} \frac{1}{1 - a_p p^{-s}} \cdot \prod_{p\not|\Delta} \frac{1}{1 - a_p p^{-s} + p^{1-2s}}$$

The BSD conjecture states that the order of this function at $s = 1$ is equal to the algebraic rank, i.e. the analytic rank is equal to the algebraic rank of the elliptic curve. It is reasonable that if the algebraic rank is large, then the number of solutions N_p should be large, compared to $p - 1$, and so the a_p would be more likely to be negative. We refer to this as the bias of the a_p.

The recently proved Sato-Tate conjecture says that the sequence $\left\{\frac{a_p}{2\sqrt{p}}\right\}$ is uniformly distributed in the interval $[-1, 1]$. Thus, the standard L-function will not necessarily detect this bias of the a_p.

To detect this bias and try to connect it to the rank of the elliptic curve, I instead look at the modified L function:

$$\tilde{L}(E,1) = \prod \left(1 - \frac{sgn(a_p)}{p}\right)^{-1}.$$

Because the rank of an elliptic curve is difficult to compute directly and the a_p are relatively easy to compute, it would be helpful to be able to determine the rank of an elliptic curve using only the a_p. My work consists of the following elements:

- Creating an algorithm in the software program SAGE that computes the product $\tilde{L}(E,1)$ for primes $p \leq X$ for increasing X.
- Examining the ratio of the number of a_p that are negative to the number that are positive

- Determining a function that correlates the rank of the elliptic curve to the ratio of the negative to positive a_p, depending on X.
- Proving that the product $\tilde{L}(E,1)$ converges and finding a heuristic determining to what function the product is asymptotically equivalent.

3. Future Research

3.1. **Twisted Elliptic Curves.** Given an elliptic curve E, one can also study the twisted elliptic curve E_d. Performing a quadratic twist of the elliptic curve, one multiplies y^2 in the equation fro E by d. By studying various twists of an elliptic curve, one may be able to say more about the distribution of the a_p's for both the original elliptic curve E and the twist E_d.

3.2. **Bounding the Error of $\tilde{L}$.** It would be useful to know how quickly the product of $\tilde{L}$ converges to its value up to a certain number of decimal places. By looking at the sum $\log \tilde{L}$, we can bound the higher order terms involving p^{-n} for $n \geq 2$ to determine a rough error bound for the desired product.

3.3. **Involving Undergraduates.** The two new projects listed could involve undergraduates, as many of the principles involved deal with real and complex analysis that they are learning. Further, the group structure of an elliptic curve gives a new perspective on basic group theory and finitely generated groups.

4. Summary

A significant part of number theory, and specifically algebraic number theory, deals with the arithmetic of elliptic curves. The use of elliptic curves spans number theory, cryptography, algebraic geometry and even dynamical systems and other areas of mathematics. Determining the structure of an elliptic curve, and specifically the algebraic rank, can be difficult. My research involves determining the rank of an elliptic curve using easily computable local data for the curve. In developing an algorithm and several examples, undergraduate students could be easily incorporated into the project.