A Weil Conjectures' Exposition

With Application to Elliptic Curves

Jafari Mohammad Mahdi

Under Supervision of Prof. Simon Serovajsky

June 24, 2025

Outline

Background

Results

L-series and Weil Conjectures

Problem Statement

We study the growth of the 2-Selmer ranks for families of elliptic curves with a rational 2-torsion. Our goal is to determine the boundedness of the Selmer ranks through its algorithmic computation using existing methods.

Elliptic Curves

Definition: *Elliptic Curve*

An *Elliptic Curve* is a projective variety of genus 1 which can be represented as

$$E : y^2 = x^3 + Ax + B$$

and over rational numbers has the structure of a free Abelian group

$$E(\mathbb{Q}) \cong E_{Tors} \oplus \mathbb{Z}^r$$

Isogeny and Torsions

Given a curve with a known, non trivial torsion group E_{Tors}, we can find a morphism of elliptic curves $\varphi : E \to E'$ which has the kernel E_{Tors}.
In this work we consider the curves for which the torsion group has the form $\{O, (r, 0)\}$ where r is any integer.

Galois Cohomology

Given the following short exact sequence

$$0 \longrightarrow E(\mathbb{Q})[\varphi] \longrightarrow E(\mathbb{Q}^{ac}) \longrightarrow E(\mathbb{Q}^{ac}) \longrightarrow 0$$

Where $E(\mathbb{Q})[\varphi]$ denotes the kernel of φ, applying the Galois cohomology we can get the sequence

$$0 \longrightarrow E(\mathbb{Q})/\varphi(E(\mathbb{Q})) \longrightarrow H^1(\mathbb{Q}, E[\varphi]) \longrightarrow H^1(\mathbb{Q}, E)[\varphi] \longrightarrow 0$$

Selmer Groups

For each prime p, consider the localization of the Galois cohomology $H^1(\mathbb{Q}_p, \cdot)$, which agrees with l-adic cohomology class. We define the Selmer group as

$$Sel^{\varphi}(E/\mathbb{Q}) = Ker\big(H^1(\mathbb{Q}, E[\varphi]) \to H^1(\mathbb{Q}_p, E)[\varphi]/H^1_{\varphi}(\mathbb{Q}_p, E)\big)$$

For each prime, where

$$H^1_{\varphi}(\mathbb{Q}_p, E) = \delta_p(E'(\mathbb{Q}_p)/\varphi(E(\mathbb{Q}_p)))$$

Is the image of the local connecting homomorphisms

Rank Problem

Generally, no algorithm is known for computation of the rank of an elliptic curve. However, we have the followin formula

$$rank(E) \leq dim(Sel^{\varphi}(E)) + dim(Sel^{\varphi'}(E')) - 2$$

where the right side is called the *Selmer Rank*.

Main Results

The main result of our research in this thesis culminates in the following theorem:

Theorem

In a family of elliptic curves with an integer 2-torsion of height $0 \leq h \leq X$, the upper bound for Selmer ranks grows as $\log \log X$.

Method

To construct the Selmer groups, we use the algorithm provided in the works of Goto for construction of the connecting homomorphisms δ_p. We then provide statistical arguments regarding the distribution of prime numbers and likelyhood of higher Selmer ranks to prove the main theorem.

Rank Problem

For the ranks of the elliptic curves we have the following conjecture

Conjecture: Beilinson-Bloch-Kato

Given an elliptic curve E with an L-function $L(E, s)$, we have the following:

$$ord_{s=1} L(E, s) = dim_{\mathbb{Q}_l} H^1_{\varphi}(\mathbb{Q}, E_l)$$

The specialized case of this conjecture for elliptic curves is the Birch-Swinnerton Dyer conjecture.

This is known in case of ranks 0 and 1. The family presented here is a natural candidate for explorations beyond the known cases.
We now discuss the construction and properties of the L-functions.

Cohomology Classes

In the first chapters of The work, we define the cohomology classes for varieties as maps $H^i : Proj(k)^o \rightarrow Vect(K)$, smooth projective varieties to finite K Vector spaces such that for an n dimensional variety, $H^i = 0$ for $i < 0$, $2n < i$. The second chapter of the work is devoted to construction of such object, and its computation.

Fixed Points

For a mapping of varieties $f\colon Y \to X$, we naturally have a map of cohomology classes $f^* : H^i(X) \to H^i(Y)$. In the work we prove the following:

$$Fixed(f) = \sum_{i=0}^{2n} (-1)^i Tr(f^* H^i(X))$$

L-functions

Now consider the finite field endomorphism $Frob_q : x \to x^q$. The local L-function of a curve now has the form

$$L_p(X, s) = \prod det(1 - tFrob_p | H^i(X))^{(-1)^{i+1}}$$

Proving this formula is the goal of the first three chapters of the presented work.

Publication

This result has been presented in the IMMM April conference 2025, and is set for publication in the Kazakh Mathematical Journal.

Conclusion

This research contributes to the understanding of the arithmetical structure of the elliptic curves and their L-functions. Using concrete computational methods and abstract theory of L-functions, this work provides the foundation for future works towards many open problems such as BSD and BBK conjectures.