V5A1: AVANCED TOPICS IN ALGEBRA: INTRODUCTION TO ARITHMETIC OF ELLIPTIC CURVES

The arithmetic of elliptic curves is a fascinating and deep subject in mathematics where algebraic geometry, number theory and analysis interplay with each other in an essential way. This course will emphasize the algebraic aspects of the theory, and it consists of two parts. The first part is a systematic introduction to some "common sense" on elliptic curves. I will start with some general facts on elliptic curves over general fields, such as Weierstrass equations, j-invariants, group law on an elliptic curves, structure of endomorphism rings, and Weil pairing. Then I want to discuss special properties of elliptic curves over various fields used in number theory: finite fields, local fields and number fields. Especially, I will give a proof of Mordell-Weil theorem, which plays a fundamental role in the arithmetic study of elliptic curves. During the proof, we define Selmer groups and Tate-Shaferevich groups of an elliptic curve over a number field, and introduce the Néron-Tate height.

The style of the second part of the course is more expository, which means that we will emphasize the understanding of basic concepts and their interactions rather than the details of proofs. In this part, we will focus on elliptic curves defined over $\mathbb{Q}$. I will start with the definition of the Hasse-Weil L-function of an elliptic curve over $\mathbb{Q}$, and its connection with modular forms and modular curves. Then I will state the BSD conjecture for elliptic curves over $\mathbb{Q}$. Next, we will discuss some basic facts on elliptic curves with complex multiplication, and define Heegner points. I will try to state (without proofs) the Gross-Zagier formula, which relates the central derivative of the L-function of an elliptic curve and the height of its Heegner points. Finally, if time allows, I want to discuss Kolyvagin's method of bounding Selmer groups and Shafarevic-Tate groups using Heegner points in the rank 0 and rank 1 case.

Prerequisite:

- A first course on algebraic geometry, especially the theory of algebraic curves.
- Algebraic number theory, especially the structures of local fields as well as their Galois groups, the Hermite-Minkowski finiteness theorem. Although I will review its basic definitions and properties, it is useful to know Galois cohomology before the course.

References:

- J. Silverman, *The Arithmetic of Elliptic Curves*, GTM **106**, Springer-Verlag, 1986.
  This is the standard reference for the first part of the course.

- J. P. Serre, *Lecture on Mordell-Weil Theorem*, 3rd edition, Springer Fachmedien Wiesbaden, 1997.
  As the title indicates, this book is a good reference for heights and Mordell-Weil theorem. Moreover, it also contains many interesting applications of heights to approximation problem and inverse Galois problem.

- N. Koblitz, *Introduction to Elliptic Curves and Modular Forms*, Second Edition, GTM **97**, Springer-Verlag, 1993.
  A good introduction to Hasse-Weil L-function.

- B. Gross, Heegner points on $X_0(N)$, in *Modular forms*, edited by Rankin, Chichester, Ellis Horwood, 1984, 87-106.

- B. Gross, Kolyvagin's work on modular elliptic curves, in *L-functions and Arithmetic, Proceedings of the Durham Symposium, July, 1989*, J. Coates and R. Taylor (eds.), London Mathematical Society Lecture Note Series, **153**. Cambridge University Press, 1991.
  This article is a very good introduction to Kolyvagin's method.