2026 Spring Elliptic Curves

Zhuoyang Liu

2026/1-2026/2

Abstract

Elliptic curve is a very important object in various fields of mathematics: in algebraic geometry, we count genus, in complex analysis, we integrate double-periodic functions, in cryptography, we construct collisions by parings, while in number theory, we build connections between algebraic and analytic aspects. This course covers some basic facts about elliptic curves on various kinds of fields and some key theorems like Mordell-Weil. The definition of L functions will also be included. By the end of the course, I will briefly introduce the famous conjecture by Birch and Swinnerton-Dyer.

●**Language**: Mainly English.

●**Schedule**: The course will last for 17 weeks with 3 class periods per week.

●**Content**:

1. **Chapter 1**—Basic Facts about Elliptic Curves

   (a) Complex Integration and Complex Torus

   (b) Weierstrass Equation and Group Structure

   (c) Tate Module

   (d) Weil Pairing

   (e) $\mathrm{End}(E)$ and $\mathrm{Aut}(E)$

2. **Chapter 2**—Elliptic Curves in Finite Fields

   (a) Counting Points

   (b) Preliminaries about Formal Groups

   (c) Good and Bad Reduction

3. **Chapter 3**—$\mathbb{Z}$, $\mathbb{Q}$ and Their Completion

   (a) From Finite to Local

   (b) NOS Criterion

   (c) Something about Group Cohomology

   (d) Height Functions

   (e) Kummer Pairing

   (f) Weak Mordell-Weil

Remark *This content is only for reference, which may be slightly different from the real class.*

References

[1] F. Diamond and J. Shurman, *A first course in modular forms.* Grad. Texts in Math., 228 Springer-Verlag, New York, 2005. xvi+436 pp. ISBN:0-387-23229-X

[2] A. Knapp, *Elliptic curves.* Math. Notes, 40 Princeton University Press, Princeton, NJ, 1992. xvi+427 pp. ISBN:0-691-08559-5

[3] J. Milne, *Elliptic curves.* Second edition [of MR2267743] World Scientific Publishing Co. Pte. Ltd., Hackensack, NJ, [2021], ©2021. x+308 pp. ISBN:[9789811221859] ISBN:[9789811221835]

[4] J. Silverman, *The arithmetic of elliptic curves.* Grad. Texts in Math., 106 Springer-Verlag, New York, 1992. xii+400 pp. ISBN:0-387-96203-4

[5] J. Silverman, *Advanced topics in the arithmetic of elliptic curves.* Grad. Texts in Math., 151 Springer-Verlag, New York, 1994. xiv+525 pp. ISBN:0-387-94328-5

[6] J. Silverman and J. Tate, *Rational points on elliptic curves.* Undergrad. Texts Math. Springer-Verlag, New York, 1992. x+281 pp. ISBN:0-387-97825-9

Remark [3] *and* [4] *are recommended to be the main textbooks.*