National Center for Theoretical Sciences

Elliptic Curves over Finite Fields and Applications to Cryptography

Time 9:50-15:40, September 2-4, 2026

Venue Room 515, Cosmology Building, NTU

Registration

Speakers | **Pin-Chi Hung** Soochow University
Jia-Wei Guo Soochow University
Tse-Chung Yang Soochow University

Organizer | **Ming-Lun Hsieh** National Taiwan University

Introduction & Purposes

This mini-course explores the arithmetic of elliptic curves over finite fields. Designed for students with a foundational background in abstract algebra, the curriculum transitions systematically from Weierstrass equations and group laws to isogenies, Vélu's formulas, and curve classification. Our primary objective is to equip students with the essential mathematical foundations required for isogeny-based cryptography. This mini-course serves a preparatory course for the incoming NCTS lecture series "Elliptic Curves in Mathematical Cryptography" given by Professor Yusuke Aikawa.

Outline & Descriptions

Day One: For Lecture 1 and Lecture 2, read Chapters I.1, I.2, III.1, III.2, and III.6, which cover projective planes, Weierstrass equations, the group law, and the general torsion structure.

Day Two: For Lecture 3 and Lecture 4, focus on Chapters III.4 and III.5, which establish the geometry of morphisms, the definition of isogenies, and the role of the kernel. See [DF10, §8.1] and [Was08, §12.3] for Vélu's formulas.

Day Three: For Lecture 5 and Lecture 6, read Chapters III.4, III.5, III.9, V.1, V.2, and V.3, which cover the endomorphism ring, the Frobenius endomorphism, Hasse's theorem, and the classification of ordinary versus supersingular curves over finite fields. For isogeny-based cryptograpy, read [DF17] for a survey.

Prerequisites

Preliminary knowledge about algebra.

Contact Murphy Yu murphyyu@ncts.tw