Spring semester 2026

Universitat Politècnica de Catalunya
Universitat Autònoma de Barcelona
Universitat de Barcelona

Barcelona Number Theory Study Group

ISOGENIES BETWEEN REDUCTIONS OF PAIRS OF ELLIPTIC CURVES

Reference person: Martín Sombra, `martin.sombra@icrea.cat`

Venue: Fridays 11:15 – 12:45, room iC at UB

The goal of the study group for this Spring semester will be to understand the article *Exceptional isogenies between reductions of pairs of elliptic curves* by François Charles [Cha18]. On the path, there will be preliminary talks dealing with the many techniques appearing in the paper, including reductions of elliptic curves, modular curves and arithmetic intersection theory on them. No previous expertise in these topics is required.

Contents

A USER GUIDE

Every section of these notes concerns a talk for the learning seminar and, after a quick presentation of the main subject of the lecture, it features a **"Condensed abstract"** and a **"Tips"** paragraph. The first one is intended to be a one-sentence motto for the lecture, containing the primary goal that the speaker should aim to for a successful talk. The second one is a collection of suggestions intended to guide the speaker in the preparation of their exposition: as long as the goal is accomplished and the time schedule respected (1h30 per talk), the final choice of propositions, examples and proofs to present is left to their taste, as well as the depth of details.

The participants are free to choose their favorite references among those proposed (or further ones!); however, for a better global coordination, it is suggested to stick to the notation of [Cha18]. The organizer stays at disposal for discussions on how to organize any specific lecture or for any doubts concerning the outlines of the talks given here. This document is available online at `https://www.ub.edu/nt/ffite/Seminars.html`.

Welcome session (06.03, *Martín Sombra*)

The goal of this first meeting is to give a presentation of the study group, sum up the contents of the talks and agree on a planned schedule among participants by finding an answer to the question "Who talks when?". Whoever is interested in participating to the learning seminar is heartily invited and will be warmly welcomed. However, for a fruitful participation to the lectures, some previous knowledge in algebra, algebraic geometry and number theory is recommended.

1. Elliptic curves over finite fields (20.03, *Oriol Navarro*)

The main result of [Cha18] concerns the reductions modulo primes of an elliptic curve over a number field. Hence a first step towards this goal is to understand the properties of elliptic curves over finite fields. The aim of this first talk is to explain the classification of such curves into ordinary and supersingular, together with the equivalent formulations of these conditions in terms of torsion points, rings of endomorphism and formal groups. We will also discuss isogenies of elliptic curves over a finite field and Tate's theorem determining isogeny pairs of elliptic curves in terms of Frobenius traces.

Condensed abstract: here we discuss the types (ordinary, supersingular) of elliptic curves over finite fields and Tate's isogeny theorem.

Tips: we primarily intend to cover Theorem V.3.1 with its proof from [Sil09] and the statement of Tate's theorem following [Sil09, Theorem III.7.7 and Exercise 5.4]. This involves presenting the necessary preliminaries on elliptic curves and their Tate's modules, formal groups and endomorphism rings from [Sil09, Chapters III, IV and V].

2. The modular curve $X(1)$ and Hecke correspondences (10.04, *Francesc Pedret*)

Condensed abstract: this is a presentation of the basic elements of the theory of modular functions for the full modular group $\Gamma(1)$ including the Petersson inner product on them. This will also include a discussion of Hecke correspondences on the modular curve $X(1)$ and its relation with isogenies of elliptic curves.

Tips: the speaker can give an account of [Sil94, Chapter 1], explaining the main material from Sections 1, 2, 3, 7, 8 and 9, plus Exercise 1.22.

3. The line bundle of modular forms (17.04, *Pip Goodman*)

Condensed abstract: here we discuss the line bundle L of modular forms of weight 12 on $X(1)$, including its global sections and the singular Hermitian metric on it induced by the Petersson inner product. Time permitting, we will also discuss the integral model $(\mathscr{X}(1), \mathscr{L})$ of the pair (X, L).

Tips: to be done.

4. Arakelov geometry on arithmetic surfaces (24.04, *Xevi Guitart*)

Arakelov geometry is an arithmetic analogue of classical algebraic geometry that compactifies schemes over the integers by adding infinite data via Hermitian metrics. It enables intersection theory and height functions in arithmetic, leading to Diophantine results like the Faltings' theorem or the proof to the Bogomolov conjecture.

The aim of this talk is to explain arithmetic surfaces and singular Hermitian line bundles on them, and show how the associated heights are defined.

Condensed abstract: The basic elements of Arakelov geometry are presented for their application in the modular setting.

Tips: this talk has to cover the material in [Aut03, Section 1] on singular Hermitian line bundles on arithmetic surfaces. This is a short account of the more sophisticated presentation in [Bos99, Section 5]. To prepare this, one might also consult [Sou21] for the classical (nonsingular) setting together with more examples and intuition.

5. The height of Hecke correspondences (08.05, *Francesc Fité*)

The strategy for the proof of the main theorem of [Cha18] starts with Autissier's computation of the height of the Hecke correspondence divisor T_N on $\mathscr{X}(1) \times_{\mathrm{Spec}(\mathbb{Z})} \mathscr{X}(1)$. This talk will present this computation together with the resulting estimate for the height intersection of an arithmetic curve with this divisor.

Tips: this talk should cover the material from [Aut03, Section 3] or from the alternative presentation in [Coh84], and use this to derive [Cha18, Corollary 2.2].

6. Equidistribution of Hecke orbits (15.05, *Roberto Gualdi*)

The aim of this talk is to explain the archimedean equidistribution theorem of Clozel, Oh and Ullmo on the modular curve.

Tips: this can be based on Sections 2.1 and 2.2 of [CU04].

7. Local statements (22.05, *Marc Masdeu*)

This talk starts the technical core of [Cha18]. In this talk we will cover two key results about the distribution of Hecke orbits, weaker than the Clozel-Oh-Ullmo equidistribution but the valid for any place (either archimedean or non-archimedean) of the number field.

Tips: the aim is to explain Propositions 3.1 and 3.2 from [Cha18] following Section 4 in this paper.

8. Separation results for Hecke orbits (29.05)

This talk discuss the final ingredient for the proof, a statement showing that there are not too many Hecke orbits that contain a very good approximation of a given point.

Tips: here we explain Proposition 3.3 of [Cha18] following Section 5 in this paper.

9. Piecing up – proof of the theorem and consequences (05.06, *Santi Molina*)

At this point, all the necessary preliminary notions and results should be in place to prove the main result about isogenies of reductions of pairs of elliptic curves [Cha18, Theorem 1.1] and its consequence concerning the structure of the reductions an elliptic curve [Cha18, Corollary 1.2].

Tips: this talk should cover [Cha18, Section 3].

10. Generalizations and/or related results (12.06, *Enric Florit*)

This final talk can be used to either discuss the generalization to abelian varieties and K3 surfaces, or to present related results like the existence of infinitely many supersingular primes for elliptic curves over a number field K admitting a real place.

Tips: the presentation of the generalizations to abelian varieties and K3 surfaces can be done following the survey paper [ST25] and the references therein. The existence of infinitely many supersingular primes when $K = \mathbb{Q}$ is proven in [Elk87] and its generalization to any K admitting a real embedding is in [Elk89].

References

[Aut03] Pascal Autissier, *The height of Hecke correspondences*, Bull. Soc. Math. Fr. **131** (2003), no. 3, 421–433.

[Bos99] J.-B. Bost, *Potential theory and Lefschetz theorems for arithmetic surfaces*, Ann. Sci. Éc. Norm. Supér. (4) **32** (1999), no. 2, 241–312.

[Cha18] François Charles, *Exceptional isogenies between reductions of pairs of elliptic curves*, Duke Math. J. **167** (2018), no. 11, 2039–2072.

[Coh84] Paula Cohen, *On the coefficients of the transformation polynomials for the elliptic modular function*, Math. Proc. Camb. Philos. Soc. **95** (1984), 389–402.

[CU04] Laurent Clozel and Emmanuel Ullmo, *Uniform distribution of Hecke points*, Contributions to automorphic forms, geometry, and number theory. Papers from the conference in honor of Joseph Shalika on the occasion of his 60th birthday, Johns Hopkins University, Baltimore, MD, USA, May 14–17, 2002, Baltimore, MD: Johns Hopkins University Press, 2004, pp. 193–254 (French).

[Elk87] Noam D. Elkies, *The existence of infinitely many supersingular primes for every elliptic curve over* $\mathbb{Q}$., Invent. Math. **89** (1987), 561–567 (English).

[Elk89] ———, *Supersingular primes for elliptic curves over real number fields*, Compos. Math. **72** (1989), no. 2, 165–172.

[Sil94] Joseph H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Grad. Texts Math., vol. 151, New York, NY: Springer-Verlag, 1994.

[Sil09] ———, *The arithmetic of elliptic curves*, 2nd ed. ed., Grad. Texts Math., vol. 106, New York, NY: Springer, 2009.

[Sou21] Christophe Soulé, *Arithmetic intersection*, Arakelov geometry and diophantine applications. Based on lectures given at the summer school, Grenoble, France, June 12–30, 2017, Cham: Springer, 2021, pp. 9–36.

[ST25] Ananth N. Shankar and Yunqing Tang, *Reductions of abelian varieties and K3 surfaces*, J. Number Theory **270** (2025), 122–166 (English).