

BARCELONA NUMBER THEORY STUDY GROUP

---

**ISOGENIES BETWEEN REDUCTIONS  
OF PAIRS OF ELLIPTIC CURVES**

---

**Reference person:** Martín Sombra, [martin.sombra@icrea.cat](mailto:martin.sombra@icrea.cat)

**Venue:** mostly Fridays 11:15 – 12:45 in room T1 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

Welcome session (06.03, <i>Martín Sombra</i> )	2
1. Elliptic curves over finite fields (20.03, <i>Oriol Navarro</i> )	2
2. The modular curve $X(1)$ and Hecke correspondences (10.04, <i>Francesc Pedret</i> )	2
3. Arakelov geometry on arithmetic surfaces (24.04, <i>Xevi Guitart</i> )	3
4. The line bundle of modular forms (08.05, <i>Pip Goodman</i> )	3
5. The height of Hecke correspondences (15.05, <i>Francesc Fité</i> )	3
6. Equidistribution of Hecke orbits (29.05, <i>Roberto Gualdi</i> )	3
7. Local statements (29.05, <i>Marc Masdeu</i> )	4
8. Bounding the best approximations (05.06, <i>Santi Molina</i> )	4
9. Piecing up – proof of the theorem and consequences (12.06, <i>Martín Sombra</i> )	4
10. Generalizations and related results (19.06, <i>Enric Florit</i> )	4
References	4

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 a discussion of Hecke correspondences and their relation with isogenies of elliptic curves.

**Tips:** the speaker can give an account of [Sil94, Chapter 1] explaining the material from Sections 2, 3, 4, 9 and 10, including Theorems 2.5, 4.1 and 9.1, and Propositions 3.7 and 10.1.

### 3. 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:** a suitable account of the Arakelov geometry for singular Hermitian line bundles on arithmetic surfaces can be found in [Kuh01, Sections 2 and 3]. The presentation should include the definition of Hermitian line bundles on arithmetic surfaces and their arithmetic intersection numbers (Theorem 2.6) and their extension to logarithmically singular metrics (Theorem 3.8). This extension is applied to define heights and prove the arithmetic Bézout formula in [Aut03, Proposition 1.4].

To prepare it, one might also consult [Sou21] for the classical (nonsingular) setting, and [Bos99] for an alternative presentation of Arakelov geometry in the singular setting.

### 4. THE LINE BUNDLE OF MODULAR FORMS (08.05, *Pip Goodman*)

Modular forms can be interpreted as global sections of line bundles on the modular curve  $X(1)$ . In this talk we will review this interpretation by introducing the line bundle  $L$  of modular forms on  $X(1)$ . We will also discuss the associated (singular) Hermitian line bundle  $\overline{\mathcal{L}}$  on the integral model  $\mathcal{X}(1)$  of the modular curve, which will provide us with a suitable setting where one can apply the techniques of Arakelov geometry.

**Tips:** this talk can be based on [Kuh01, Section 4] focussing on the construction in Section 4.12 of the singular Hermitian line bundle  $\overline{\mathcal{L}}$  for  $\Gamma = \Gamma(1)$ . This should also include Proposition 4.7 and 4.9, and Remark 4.10. To this end one might also consult [DI95], in particular its Section 12.1.

### 5. THE HEIGHT OF HECKE CORRESPONDENCES (15.05, *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  $\mathcal{X}(1) \times_{\text{Spec}(\mathbb{Z})} \mathcal{X}(1)$ . This talk will present this computation together with the resulting estimate for the height of the intersection of an arithmetic curve with this divisor.

**Tips:** this talk should cover [Aut03, Section 3] focussing on Theorem 3.2 and its proof. Applying this result we will derive the estimate in [Cha18, Corollary 2.2] for the intersection of a horizontal curve in  $\mathcal{X}(1)$  with the Hecke orbits of another such curve.

Time permitting, it would be nice to include Kuhn's computation of the height of the modular curve (Proposition 3.1) using the modular Jensen's formula due to Rorhlich [Roh84].

### 6. EQUIDISTRIBUTION OF HECKE ORBITS (29.05, *Roberto Gualdi*)

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

**Tips:** this talk can be based on Sections 2.1 and 2.2 of the paper [CU04]. The aim is to present Theorem 2.1, with emphasis on the qualitative statement (c). Its proof is based on the spectral

theory on the modular curve and on results in the direction of the Ramanujan–Petterson conjecture. For these subjects one might also consult the book [Iwa95].

#### 7. LOCAL STATEMENTS (29.05, *Marc Masdeu*)

This talk starts the technical core of [Cha18]. Here we will cover two key results about the distribution of the Hecke orbits in the non-archimedean setting: the first deals with the places of bad reduction, and the second is a weak form of the Clozel-Oh-Ullmo equidistribution.

**Tips:** the aim of this talk is to explain Propositions 3.1 and 3.2 from [Cha18] following Section 4 in this paper. For the proof of the auxiliary Proposition 4.1 one might alternatively follow [Sil90, Proposition 2.1].

#### 8. BOUNDING THE BEST APPROXIMATIONS (05.06, *Santi Molina*)

This talk discusses the final ingredient of 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 (12.06, *Martín Sombra*)

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 of an elliptic curve [Cha18, Corollary 1.2].

**Tips:** this talk should cover the material in [Cha18, Section 3].

#### 10. GENERALIZATIONS AND RELATED RESULTS (19.06, *Enric Florit*)

In this final talk we can either discuss the generalization of the presented results to abelian varieties and K3 surfaces, or present related results like the existence of infinitely many supersingular primes for elliptic curves over a number field  $K$  admitting a real embedding.

**Tips:** the generalizations to abelian varieties and K3 surfaces can be prepared 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] Jean-Benoît 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.
- [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).

- [DI95] Fred Diamond and John Im, *Modular forms and modular curves*, Seminar on Fermat's Last Theorem (Toronto, ON, 1993–1994), CMS Conf. Proc., vol. 17, Amer. Math. Soc., Providence, RI, 1995, pp. 39–133. MR 1357209
- [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.
- [Iwa95] Henryk Iwaniec, *Introduction to the spectral theory of automorphic forms*, Biblioteca de la Revista Matemática Iberoamericana, Revista Matemática Iberoamericana, Madrid, 1995.
- [Kuh01] Ulf Kuhn, *Generalized arithmetic intersection numbers*, J. Reine Angew. Math. **534** (2001), 209–236.
- [Roh84] David E. Rohrlich, *A modular version of Jensen's formula*, Math. Proc. Cambridge Philos. Soc. **95** (1984), no. 1, 15–20.
- [Sil90] Joseph H. Silverman, *Hecke points on modular curves*, Duke Math. J. **60** (1990), no. 2, 401–423.
- [Sil94] ———, *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).