# MODULI PROBLEMS OF ELLIPTIC CURVES
# TERM 1 STUDY GROUP, 2023-24

ELVIRA LUPOIAN

The main aim of this study group is to understand the foundations of the arithmetic theory of moduli spaces of elliptic curves. The classical references on this subject are the 1972 paper of Deligne and Rapoport [1] and the 1985 work of Katz and Mazur [2]. Both sources approach the problem from different perspectives, the former making heavy use of the language of stacks, whilst the latter focuses on the study of relatively representable moduli problems. Our study group will focus on the work of Katz and Mazur.

## 1. Introduction

**Category of Elliptic Curves.**

**Definition 1.1.** Let $K$ be an algebraically closed field. An elliptic curve over $K$ is a pair $(E, O)$, where $E$ is a genus 1 curve, which is proper, connected, smooth over $K$, and $O \in E(K)$ is a marked $K$-rational point.

We recall two basic facts about any such elliptic curve $(E, O)$:

1. E has a natural group scheme structure;
2. E can be embedded in $\mathbb{P}^2_K$ via a generalised Weierstrass equation.

**Definition 1.2.** Let $S$ be a scheme. An elliptic curve over $S$ is a pair $(E \to S, O)$, consisting of a morphism of schemes $E \to S$, which is proper, smooth and it's fibers are connected curves of genus 1; and $O \in E(S)$ is a section.

We usually denote such an elliptic curve $(E \to S, O)$ by $E/S$.

We can view such a curve as a "family" of elliptic curves, since any point $x \in S$ defines an elliptic curve $E_x$ over the residue field $K(x)$.

**Example 1.3.** Let $R = \mathbb{Z}[j, 1/j, 1/(1728 - j)]$. Then

$$y^2z + xyz = x^3 - \frac{36}{j-1728}xz^2 - \frac{1}{1-1728}z^3$$

is an elliptic curve over $\operatorname{Spec}(R)$.

There are two important facts about elliptic curve over schemes proved in [2]:

1. In general, $E/S$ cannot be embedded into $\mathbb{P}^2_S$, but a local version of this holds. Namely, $E|_{U_i}$ can be embedded into $\mathbb{P}^2_{U_i}$ for some covering $\{U_i\}$ of $S$.
2. As in the previous case, elliptic curves over schemes have the structure of a commutative group scheme over the base scheme.

We will study the category of elliptic curves: $Ell$. The objects of this category are elliptic curves over schemes, and the morphism between $E/S$ and $E'/S'$ are pairs $(f : S' \to S, g : E' \to E)$ such that the corresponding diagram is Cartesian, and the section $O_{S'} : S' \to E'$ induced by $O$ equals $O'$.

*Remark* 1.4. We should note that the base scheme in the above definition is allowed to vary.

Our moduli problems will essentially be functors from this category to the category of sets. The main question will be whether these functors are representable.

**Definition 1.5.** Let $\mathcal{C}$ be a category, and $F : \mathcal{C} \to \text{Sets}$ a functor. $F$ is representable if there exists an object $X \in \text{Ob}(\mathcal{C})$ such that $F \simeq h^X$, isomorphic as functors, where $h^X$ is the functor

$$h^X : \mathcal{C} \to \text{Sets}, T \mapsto \text{Hom}(T, X).$$

The object $X$ is callled the representing object of $X$.

**Moduli Problems.**

**Definition 1.6.** A moduli problem of elliptic curves is a contravariant functor

$$P : Ell \to \text{Sets}$$

Let $P$ be any moduli problem of elliptic curves. To any $E/S \in \text{Ob}(Ell)$, the functor associates a set $P(E/S)$. We call an element of $P(E/S)$ a $P$–structure on $E/S$, and we define $Ell_P$, the category of elliptic curves with $P$-structures as:

- Objects: $(E/S, \alpha)$ with $E/S \in \text{Ob}(Ell)$, $\alpha \in P(E/S)$
- Morphisms $\phi \in \text{Hom}((E/S, \alpha), (E'/S', \alpha'))$ are morphisms $\phi \in \text{Hom}(E/S, E'/S')$ such that $P(\phi)$ takes $\alpha$ to $\alpha'$.

We should note the existence of a forgetful functor:

$$F_P : Ell_P \to Ell, (E/S, \alpha) \mapsto E/S$$

Given a moduli problem of elliptic curves, we want to establish whether it is representable. If $P$ is a representable moduli problem of elliptic curves, and $X = E/S$ is its representing object, we will call $S$ the fine moduli scheme associated to $P$, and $E$ the universal elliptic curve over $S$.

*Remark* 1.7. For any $E/S$, the $h^{E/S}$ is trivially representable. As above, we define $Ell_{E/S} := Ell_{h^{E/S}}$, the category of elliptic curves with $h^{E/S}$ structures; and the corresponding forgetful functor $F_{E/S} := F_{h^{E/S}}$.

We introduce the weaker notion of relative representability.

**Definition 1.8.** A moduli problem $P$ is relatively representable if for any $E/S$, $P \circ F_{E/S}$ is representable.

**Theorem.** *A representable moduli problem is relatively representable.*

For any moduli problem $P$ and any $E/S$, the set of automorphisms

$$\text{Aut}(E/S) = \{g : E \to E | \pi g = g\}$$

acts on the set $P(E/S)$.

**Definition 1.9.** A moduli problem $P$ is called rigid if for any $E/S$ the above action is free.

**Definition 1.10.** Let $P$ be a relatively representable moduli problem. $P$ is called finite/affine/ étale if for any $E/S$, $S_{E/S}$ is finite/affine/ étale, where $S_{E/S}$ is the fine moduli scheme associated to $P \times h^{E/S}$.

**Theorem.** *(Katz-Mazur) Let $P$ be a relatively representable and affine moduli problem of elliptic curves. Then $P$ is representable if and only is $P$ is rigid. Furthemore, if $P$ is representable, then its fine moduli scheme $S_P$ is affine; and if $P$ is also étale then $S_P$ is a smooth curve over $\mathbb{Z}$.*

**Basic Moduli Problems.** Our studies will mainly focus on the following moduli problems.

$$[\Gamma(n)] : E/S \mapsto \{\text{iso.}\, (\mathbb{Z}/n\mathbb{Z})_S^2 \to E[n]\}$$
$$[\Gamma_1(n)] : E/S \mapsto \{\text{embeddings}\, (\mathbb{Z}/n\mathbb{Z})_S \to E[n]\}$$
$$[\Gamma_0(n)] : E/S \mapsto \{\text{subschemes of } E[n] \text{ locally isomorphic to}\, (\mathbb{Z}/n\mathbb{Z})\}$$

**Theorem.** *(Katz-Mazur) For any $n \geq 1$, $[\Gamma(n)]$, $[\Gamma_1(n)]$ and $[\Gamma_0(n)]$ are relatively representable, finite and étale. If $n \geq 4$, $[\Gamma(n)]$ and $[\Gamma_1(n)]$ are representable and their moduli schemes are smooth affine curves over Spec$\mathbb{Z}[1/n]$. For any $n \geq 1$, $[\Gamma_0(n)]$ is not rigid and hence not representable.*

*Remark* 1.11. Moduli schemes are often called affine or open modular curves. They are not proper over $\mathbb{Z}$. We'll discuss how they can be compactified in the final talk of the study group.

## 2. Outline

**Week 2: Modular Curves and Elliptic Curves over $\mathbb{C}$.** This will a straightforward introduction to modular curves as most people have seen them before. There will be a brief discussion of elliptic curves over $\mathbf{C}$ and level structures. We will then relate these to usual construction of modular curves as quotients of $\mathbb{H}^*$. Samir's notes on "Explicit Arithmetic of Modular Curves", [3] is a good reference for this talk. This talk should discuss:

- the representations of complex elliptic curves via lattices;
- quotients of the upper half plane by congruence subgroups;
- the bijection between certain quotients of the upper half planes and isomorphism classes of elliptic curves with certain torsion information.

**Reference:** [3] Chapter 3

**Week 3: Elliptic Curves over Schemes.** This talk should introduce the basic properties of elliptic curves over schemes. There are many things which can be discussed in this talk, and as we will not study elliptic curves over schemes specifically, it would be beneficial if the speaker gave an overview of Chapter 2 [2], and omitted the technical proofs. Some of the topics discussed can include:

- the groups scheme structure of $E/S$ - this is Section 2.1;
- the 'local embedding of the $E/S$ via Weierstrass equations. A detailed version of this can be found in Section 2.2 and a nice sketch of this can be found in David's book;
- the map $[N] : E \to E$, and it's scheme theoretic kernel - this is presented in Sections 2.3 - 2.7, many auxiliary results can be black-boxed.

**Reference**: [2] Chapter 2.

**Week 4: $\Gamma(n), \Gamma_1(n)$ and $\Gamma_0(n)$ structure.** This talk is based on Chapter 3 of [2]. The main focus of this talk should be to carefully define level structures on elliptic curves and motivate the technicalities which will appear in future talks. The speaker should define $\Gamma(n), \Gamma_0(n)$ and $\Gamma_1(n)$ structures. Relevant material from Chapter 1 can also be covered here. For instance, a brief discussion of Cartier divisors is relevant.

**Reference**: [2] Sections 3.1, 3.2, 3.3

**Week 5: Representability and the Category of Elliptic Curves.** In this talk we will introduce moduli problems for the first time in our study group. The speaker can begin with a brief overview of the category theory language used through the construction of moduli problems. A good reference for this is David's book, Sections (9.1) and (9.2). In particular, representable functors should be covered. As examples of representable functors, the speaker can discuss the functors defined in Section (3.6), and state the relevant results of Sections (3.6) and (3.7). The category of elliptic curves should then be introduced and moduli problems for elliptic curves can be defined at this point, Sections (4.1) - (4.3).

**Reference**: [2] Sections 3.6, 3.7, 4.1, 4.2, 4.3.

**Week 6: Properties of Moduli Problems.** This talk should define basic key properties of moduli problems such as rigidity, relative representability and other geometric properties, as in section (4.6). The theorem of section (4.7) should also be discussed, the proof is technical, and unnecessary for our study group. The corollaries are relevant, and should be covered, as well as the examples appearing throughtout this chapter. Setions (4.12) and (4.13) will also be relavant for us, and should be briefly discussed.

**Reference**: [2] (4.4) - (4.13).

**Week 7: The First Main Theorem of KM and its Consequences.** This talk will introduce the first main theorem of [2], namely that the moduli problems introduced in the previous talks are relatively representable. The proof of this is difficult, and a lot of general mechanism of Deligne is required, we will skip this. Instead, we will focus on the important consequences which can be deduced from this theorem - as presented in Sections (5.5) and (5.6).

**Reference**: [2] (5.1), (5.5) and (5.6).

**Week 8: Quotients by finite groups.** This talk is based on Chapter 7. It should give an overview of the general setting and results. The focus should be on the appications to our moduli problems, as presented in (7.4). We want to explicitly describe the actions of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ and $(\mathbb{Z}/N\mathbb{Z})^\times$ on the moduli problem $[\Gamma(N)]$ and $[\Gamma_1(N)]$ respectively, and the maps constructed in Theorem 7.4.2.

**Reference**: [2] Chapter 7.

**Week 9: Coarse Moduli Schemes.** In this talk we will define a "coarse moduli scheme". We will then define the $j$-line as a coarse moduli scheme. The speaker should follow the first sections of Chapter 8 closely.

**Reference**: [2] Chapter 8.

**Week 10: Cusps and the Tate curve.** This talk will define the scheme cusps, as in (8.6) [2]. We will also introduce the notion of "smoothness" at cusps, and discuss some of the further important results in later chapters of the book.

**Reference**: [2] Chapter 8.

## References

[1] P. Deligne and M. Rapoport. Les schémas de modules de courbes elliptiques. In *Modular Functions of One Variable II: Proceedings International Summer School University of Antwerp, RUCA July 17–August 3, 1972*, pages 143–316. Springer, 1973. (document)

[2] N. M. Katz and B. Mazur. *Arithmetic moduli of elliptic curves.* Number 108. Princeton University Press, 1985. (document), 1, 2, 2, 2, 2, 2, 2, 2, 2

[3] S. Siksek. Explicit arithmetic of modular curves. *Summer school notes*, 2019. 2