Moduli spaces of level n structures on elliptic curves

Emanuele Pavia

April 12, 2019

Abstract

In this talk I will present briefly some classical results about basic moduli problems of elliptic curves over any base. In order to give a decent view of the topic, many proofs will be just sketched; the main goal is to highlight the importance of such problems in studying arithmetic properties of elliptic curves with a certain generality, and to state the main results of representability.

It will not be assumed any confidence with the formalism of moduli problems and I will recall also the definitions of basic objects such as Cartier divisors and elliptic curves, which are well known and understood when defined over a field but quite subtle when the base is arbitrary.

Contents

1 Review of notations in the general setting 1

2 Moduli problems, fine and coarse moduli spaces 2

3 The four basic moduli problems for elliptic curves 5
- 3.1 $\Gamma(n)-$structures 5
- 3.2 $\Gamma_1(n)-$structures 6
- 3.3 Balanced $\Gamma_1(n)-$structures 6
- 3.4 $\Gamma_0(n)-$structures 7

4 Relative representability of level n moduli problems 7
- 4.1 The situation in general 7
- 4.2 The situation when n is invertible 8

5 Regularity theorem 9

6 Coverings of the moduli spaces 10

1 Review of notations in the general setting

First of all, let us recall the definition of elliptic curves and Cartier divisors in the most general setting.

Definition 1. Let S be a scheme. An *elliptic curve* over S is a one-dimensional finite type group scheme $E \longrightarrow S$ with geometrically connected fibers, such that E is smooth and proper over S.

We can gather all elliptic curves in a suitable category. Let $\mathcal{E}\mathrm{ll}$[1] be the category of elliptic curves defined in the following way: the objects are elliptic curves over an arbitrary base $E \longrightarrow S$ (that we shall denote with E/S), and the morphisms $f\colon E'/S' \longrightarrow E/S$ are cartesian commutative squares:

$$\begin{tikzcd}
E' \arrow[r, "f"] \arrow[d, "\alpha_{E'}"'] \arrow[dr, phantom, "\lrcorner", very near start] \arrow[dr, phantom, "\circlearrowleft"] & E \arrow[d, "\alpha_E"] \\
S' \arrow[r, "g"'] & S
\end{tikzcd}$$

(equivalently, an arrow in $\mathcal{E}\mathrm{ll}$ is an isomorphism $\binom{f}{\alpha_{E'}}\colon E' \xrightarrow{\cong} E \times_S S'$).

We present again the statement about the structure of the $n-$torsion of an elliptic curve E over an arbitrary base scheme S, that in class we have seen just for E defined over a field, in all its generality.

Theorem 2. *Let E be an elliptic curve defined over an arbitrary scheme S. Let $n \geq 1$ an integer. The $S-$homomorphism "multiplication by n":*

$$[n]\colon E \xrightarrow{\Delta} E^{\times n} \xrightarrow{m} E$$

is a finite, locally free of rank n^2 $S-$homomorphism. When S is defined over $\mathbb{Z}[\frac{1}{n}]$ (i.e. n is invertible in S) then the kernel $E[n]$ is a finite étale scheme over S, which is étale-locally on S isomorphic to the constant group scheme[2] *$(\mathbb{Z}/n\mathbb{Z})^2_S$.*

Proof. The result is well known when $S = \mathrm{Spec}(\mathbb{C})$, because by transcendental methods we know that E^{an} is (non-canonically) isomorphic to the quotient of $\mathbb{C}$ by a full rank lattice Λ and thus $E[n]$ is isomorphic to $(1/n \cdot \Lambda)/\Lambda$ which is a free $\mathbb{Z}/n\mathbb{Z}-$module of rank 2. The aim of the proof is to reduce to that case. Zariski locally on S, E is given by a smooth Weierstrass cubic in $\mathbb{P}^2_S$, so we can assume without loss of generality that S is the open subset $U \subsetneq \mathrm{Spec}(\mathbb{Z}[a_1, \dots, a_5])$ where $y^2 + a_1xy + a_2y = x^3 + a_3x^2 + a_4x + a_5$ is smooth.

---

[1] This is what Deligne calls *modular stack* in [1].

[2] For an abstract group G, the constant group scheme G_S is just the disjoint union of $\#G$ copies of the base scheme S, whose multiplication is given by the natural action of G.

In this way, S is regular and then since the structural morphism $E \longrightarrow S$ is smooth is also regular.
Let us now concentrate on the multiplication by n morphism. If it is finite, it is a finite morphism between regular schemes of the same dimension, so it is automatically flat, hence we only need to prove the finiteness. It is proper, because E is proper over S and $[n]$ is an $S-$homomorphism. We are only left to prove, geometric fiber by geometric fiber over S, that $[n]$ has finite fibers: let us suppose E is defined over an algebraically closed field k. Since any morphism between proper smooth connected curves over $k = \bar{k}$ is either finite flat or constant, and since $[n]$ is not constant (just take m coprime both with n and $char(k)$), and then one sees immediately that $[n]$ induces an automorphism on the m^2 points of order m of $E(k)$) it follows that has to be finite flat.
Finally, let us consider the case when n is invertible in the base S. Then over S the morphism $[n]$ is finite flat and fiber by fiber étale (on every point, the tangent map at the origin induced by $[n]$ is the ordinary multiplication by n which is an isomorphism in our hypothesis), and thus it is étale. Now on $S[\frac{1}{n}]$, being normal and connected, to show that $E[n]$ is a twisted $(\mathbb{Z}/n\mathbb{Z})^2_S$ it suffices to do so at a single geometric point of $S[\frac{1}{n}]$: just take a $\mathbb{C}-$valued point of S and the claim follows. ☐

Corollary 3. *Let S be an arbitrary scheme, E an elliptic curve over S, $n \geq 1$ an integer. If $E[n]$ is finite etale over S then n is invertible on S.*

Proof. The map $[n]$ is an f.p.p.f. $E[n]-$torsor. If $E[n]$ is finite étale over S, the map $[n]$ is also finite étale and thus it induces an isomorphism over the Lie algebra of E, where it is just the multiplication by n. It follows that n must be invertible in $\mathscr{O}_S$. ☐

This structure theorem will be important in defining the level n moduli spaces in the following sections.

2 Moduli problems, fine and coarse moduli spaces

Definition 4. A *moduli problem* for a certain category $\mathcal{C}$ is a contravariant functor $\mathcal{P}\colon \mathcal{C}^{\mathrm{op}} \longrightarrow \mathcal{S}\mathrm{et}$.
Given X an object of $\mathcal{C}$, we shall say that an element $\alpha \in \mathcal{P}(X)$ is a *level* $\mathcal{P}$ *structure on* X.

We are mainly interested in the following problem: consider $\mathcal{S}\mathrm{ch}$ the category of all schemes, and consider the functor $\mathscr{M}_{g,n}$ sending a scheme S to the class of smooth projective curves C of genus g and with a distinct set of n $S-$points in C. For $g = 1 = n$ this is just the *moduli problem of elliptic curves.*
Is there a way to parametrize a family of elliptic curves via a universal scheme?

Definition 5.

1. Given a moduli problem $\mathcal{P}\colon \mathcal{C}^{\mathrm{op}} \longrightarrow \mathcal{S}$, we say that $\mathcal{P}$ is *representable* if there exists an object $\mathscr{M}(\mathcal{P})$ in $\mathcal{C}$ such that there exists a bijection of sets, functorial in X, between $\mathcal{P}(X)$ and $\operatorname{Hom}_{\mathcal{C}}(X,\, \mathscr{M}(\mathcal{P}))$. This $\mathscr{M}(\mathcal{P})$ is said to be a *fine moduli space* for $\mathcal{P}$;

2. An object $\mathcal{M}(\mathcal{P})$ is said to be a *coarse moduli space* for $\mathcal{P}$ if there exists a natural transformation of functors:

$$\tau\colon \mathcal{P} \overset{\cdot}{\longrightarrow} \operatorname{Hom}_{\mathcal{C}}(-,\, \mathcal{M}(\mathcal{P}))$$

   which is universal for every natural transformation from $\mathcal{P}$ to any other representable functor.

The difference between these two definitions is that a fine moduli space parametrizes not only the objects of a moduli problem, but even the morphisms between them. Of course, a fine moduli space is also a coarse moduli space.

So, let us focus again on the moduli problem $\mathscr{M}_{1,1}$. Classically (see for example [4]) this moduli problem is provided of a coarse moduli scheme $\mathcal{M}(\mathscr{M}_{1,1})$ given by the $j-$affine line $\mathbb{A}^1_j := \operatorname{Spec}(\mathbb{Z}[j])$, where j is the normalized $j-$invariant[3]. This makes $\mathbb{A}^1_j$ the main candidate to be a fine moduli space for $\mathscr{M}_{1,1}$. However, it turns out that $\mathscr{M}_{1,1}$ cannot be representable.

First of all let us introduce some notation. From now on, we shall consider moduli problems on elliptic curves, i.e. moduli problems on $\mathcal{E}\,\mathrm{ll}$. In the case $\mathcal{P}$ is a representable moduli problem, we shall denote by $\mathbb{E}/\mathscr{M}(\mathcal{P})$ the universal elliptic curve over the universal base which represents $\mathcal{P}$.

Definition 6.

1. A moduli problem $\mathcal{P}$ is *rigid* if every pair $(X,\, \alpha)$ where X is an object of $\mathcal{C}$ and α a level $\mathcal{P}$ structure on it, has no non-trivial automorphisms. This means that the group $\operatorname{Aut}(X)$ acts freely on $\mathcal{P}(X)$.

2. A moduli problem $\mathcal{P}$ is *relatively representable* if given any E/S elliptic curve over a base S, the relative functor defined over $\mathcal{S}\mathrm{ch}_{/S}$ via the assignation:

$$T \mapsto \mathcal{P}(E_T/T)$$

   is representable by an $S-$scheme $\mathcal{P}_{E/S}$.

Remark 7.

---

[3] This is self-evident, since every elliptic curve is characterized up to isomorphism by its $j-$invariant

- If $\mathcal{P}$ is representable by $\mathbb{E}/\mathscr{M}(\mathcal{P})$ then of course it is relatively representable: every $\mathcal{P}_{/S}$ relative moduli problem is represented by the $S-$scheme $\underline{\text{Isom}}_{S\times\mathscr{M}(\mathcal{P})}(\pi_1^*E,\ \pi_2^*\mathbb{E})$, where $\pi_1\colon E\times\mathbb{E}\longrightarrow E$ and $\pi_2\colon E\times\mathbb{E}\longrightarrow\mathbb{E}$ are the natural projections;

- Given $\mathcal{S}$ a representable moduli problem (say the representative is $\mathbb{E}/\mathscr{M}(\mathcal{S})$) and $\mathcal{P}$ a relatively representable moduli problem (say that $\mathcal{P}_{/S}$ is represented by $\mathcal{P}_{E/S}$), the simultaneous moduli problem
$$\mathcal{S}\times\mathcal{P}\colon E/S\mapsto\mathcal{S}(E/S)\times\mathcal{P}(E/S)$$
is representable by the $\mathscr{M}(\mathcal{S})-$scheme $\mathcal{P}_{\mathbb{E}/\mathscr{M}(\mathcal{S})}$, which we will denote by $\mathscr{M}(\mathcal{S},\ \mathcal{P})$.

Key Remark 8. It is a straightforward computation to show that if a moduli problem of elliptic curves $\mathcal{P}$ is representable by a universal elliptic curve $\mathbb{E}$ over a universal base $\mathscr{M}(\mathcal{P})$ then the base $\mathscr{M}(\mathcal{P})$ represents the functor $\mathcal{S}\text{ch}\longrightarrow\mathcal{S}\text{et}$ defined by the assignation:
$$S\mapsto\left\{\begin{matrix}(E/S,\ \alpha)\text{ such that }E\text{ is an elliptic curve over }S\\ \text{with given level }\mathcal{P}\text{ structure }\alpha\end{matrix}\right\}$$

Proposition 9. *A relatively representable moduli problem $\mathcal{P}$ which is also affine over* $\mathcal{E}\text{ll}$ *(i.e. for all E/S the structure morphism $\mathcal{P}\longrightarrow S$ is affine) is representable if and only if it is rigid. If moreover it is étale over* $\mathcal{E}\text{ll}$ *then it is representable by a smooth affine curve over $\mathbb{Z}$.*

Proof.

$\Leftarrow$ A representable functor is also a sheaf for a suitable (subcanonical) Grothendieck topology on $\mathcal{E}\text{ll}$. The existence of non-trivial automorphism implies the impossibility of glueing the relative representatives $\mathcal{P}_{E/S}$ on the fibers, and thus it contradicts the sheaf condition of the Hom functor;

$\Rightarrow$ (Sketch) One considers the simultaneous moduli problem $\mathcal{S}\times\mathcal{P}$ with $\mathcal{S}$ a representable moduli problem over $\mathbb{Z}\left[\frac{1}{2}\right]$, and the simultaneous moduli problem $\mathcal{S}'\times\mathcal{P}$ with $\mathcal{S}'$ a representable moduli problem over $\mathbb{Z}\left[\frac{1}{3}\right]$. This yields two representatives of $\mathcal{P}$ over $\mathbb{Z}\left[\frac{1}{2}\right]$ and $\mathbb{Z}\left[\frac{1}{3}\right]$, which by the rigidity of $\mathcal{P}$ agree over $\mathbb{Z}\left[\frac{1}{6}\right]$ via a unique isomorphism, which makes it possible to glue the two representatives. See [5, Scholie 4.7.0] for the full proof.

The latter claim can be found in [5, Corollary 4.7.1]. □

We have all the ingredients to show that $\mathbb{A}^1_j$ cannot be a fine moduli space. In fact, suppose $\mathscr{M}_{1,1}$ is representable by $\mathbb{A}^1_j$ (which is affine), then it has to be rigid, but it is easy to find automorphisms of elliptic curves fixing the $S-$point

of the identity (just take the morphism $x \mapsto -x$).
But the last proposition tells us something more: the representability fails exactly because of the abundance of automorphisms. (This *always* messes up the representability of a moduli problem, see for example the functor $\mathcal{P}\mathrm{ic}$). The idea is then to force morphisms to preserve additional structure, in order to rigidify the moduli problem. The additional structure we will add is given on the $n-$torsion part of E.

3 The four basic moduli problems for elliptic curves

3.1 $\Gamma(n)-$structures

Definition 10. Let $n \geq 1$ be an integer. Consider the functor

$$E/S \mapsto \{\phi\colon (\mathbb{Z}/n\mathbb{Z})^2 \xrightarrow{\cong} E[n](S)\} \tag{1}$$

. This is called the *naive level n structure moduli problem.*

By theorem 2, we know that the moduli problem defined in Definition 10 is (indeed) naive: we cannot hope to have this isomorphism if n is not invertible on the base scheme S, because an isomorphism as abstract groups would induce an isomorphism from the constant scheme $(\mathbb{Z}/n\mathbb{Z})^2_S$ to the kernel $E[n]$; but the former is always étale (trivially) while the second is not in general. In 1974, Drinfeld ([2]) came up with the correct generalization which works for every n and which agrees with the naive problem when n is invertible in S.

Definition 11. Let $n \geq 1$ be an integer. A $\Gamma(n)-$*structure* (or a *full level n structure*) on an elliptic curve E over S is a group homomorphism

$$\Phi\colon (\mathbb{Z}/n\mathbb{Z})^2 \longrightarrow E[n](S)$$

which is a generator of $E[n]$ as a Cartier divisor, i.e. there is an equality of Cartier divisors

$$E[n] = \sum_{a,b\in\mathbb{Z}/n\mathbb{Z}} [\Phi(a,\, b)]$$

The $S-$points $\Phi(1,\, 0)$ and $\Phi(0,\, 1)$ are called *a Drinfeld basis of* $E[n]$.

The moduli problem:

$$\begin{aligned} &\mathcal{E}\mathrm{ll} \longrightarrow \mathcal{S}\mathrm{et} \\ &E \mapsto \{\Gamma(n) - \text{structures on } E\} \end{aligned} \tag{2}$$

will be simply denoted with $\Gamma(n)$.

3.2 $\Gamma_1(n)-$structures

Definition 12. Let $n \geq 1$ be an integer. A $\Gamma_1(n)-$*structure* on an elliptic curve E over S (or a *point of exact order n in $E(S)$*, or a $(\mathbb{Z}/n\mathbb{Z})-$*structure* on $E[n]$) is a group homomorphism:

$$\Phi\colon \mathbb{Z}/n\mathbb{Z} \longrightarrow E[n](S)$$

such that the Cartier divisor $\sum_a [\Phi(a)]$ is a subgroup scheme of E.

The moduli problem:

$$\begin{aligned} &\mathcal{E}\mathrm{ll} \longrightarrow \mathcal{S}\mathrm{et} \\ &E \mapsto \{\Gamma_1(n) - \text{structures on } E\} \end{aligned} \tag{3}$$

will be simply denoted with $\Gamma_1(n)$.

3.3 Balanced $\Gamma_1(n)-$structures

Definition 13. Let $n \geq 1$ be an integer. A *balanced* $\Gamma_1(n)-$*structure* on an elliptic curve E over S is a diagram:

$$\begin{tikzcd} E \arrow[r, shift left, "\phi"] & E' \arrow[l, shift left, "\phi^\vee"] \end{tikzcd}$$

where E' is an elliptic curve over S, ϕ is an $n-$isogeny and $\phi^\vee$ is the dual isogeny[4], together with two generators P and P' of $\ker(\phi)(S)$ and $\ker(\phi^\vee)(S)$ respectively.

Equivalently ([3, Exp. V, 4.1]), but less symmetrically, a balanced Γ_1-structure can be seen as a f.p.p.f. short exact sequence of group schemes over S:

$$0 \longrightarrow K \longrightarrow E \longrightarrow K' \longrightarrow 0$$

such that K and K' are both locally free of rank n, together with points $P \in K(S)$ and $P' \in K(S')$ which generate K and K', respectively.

The moduli problem:

$$\begin{aligned} &\mathcal{E}\mathrm{ll} \longrightarrow \mathcal{S}\mathrm{et} \\ &E \mapsto \{\text{Balanced } \Gamma_1(n) - \text{structures on } E\} \end{aligned} \tag{4}$$

will be simply denoted with $\Gamma_1(n)$.

---

[4] Recall that this means that $\phi \circ \phi^\vee$ is the multiplication by n on E', and $\phi^\vee \circ \phi$ is the multiplication by n on E.

3.4 $\Gamma_0(n)-$structures

Definition 14. Let $n \geq 1$ be an integer. A $\Gamma_0(n)-$*structure* on an elliptic curve E over S is an $n-$isogeny $\phi\colon E \longrightarrow E'$ which is *cyclic*, i.e. f.p.p.f. locally on S the kernel $\ker\phi$ admits a generator.

The moduli problem:

$$\begin{aligned} &\mathcal{E}\mathrm{ll} \longrightarrow \mathcal{S}\mathrm{et} \\ &E \mapsto \{\Gamma_0(n) - \text{structures on } E\} \end{aligned} \tag{5}$$

will be simply denoted with $\Gamma_0(n)$.

Remark 15.

- If n can be factorized as the product of two integers p and q, where p and q are coprimes, then it is not so difficult to see that $\Gamma(n)(E/S) \cong \Gamma(p)(E/S) \times \Gamma(q)(E/S)$, and the analougous holds for all the other three functors (3), (4), (5);
- The functors (2), (3), (4) and (5) have all a relative variant defined over $\mathcal{S}\mathrm{ch}_{/S}$. Let us fix a moduli problem $\mathcal{P}$ between these ones, and let us fix an elliptic curve E/S. Then the relative functor $\mathcal{P}(E/S)$ is defined as:

$$T \mapsto \mathcal{P}\left(E_T/T\right)$$

- If E and E' are elliptic curves over a base S, and we are given an $S-$group isomorphism $E[n] \xrightarrow{\cong} E'[n]$, then we have an isomorphism of relative functors $\mathcal{P}(E/S) \cong \mathcal{P}(E'/S)$ for every $\mathcal{P}$ moduli problem among (2), (3), (4) and (5), since they obviously depend only on the structure of the kernel $E[n]$.

We want now to study the representability of these four moduli problems. By the Key Remark 8, we know that if $\mathcal{P}$ is any of the functors (2), (3), (4) or (5) and it is representable by an elliptic curve $\mathbb{E}$ over a base $\mathscr{M}(\mathcal{P})$, then the latter scheme $\mathscr{M}(\mathcal{P})$ represents the moduli problem of elliptic curves with given level $\mathcal{P}$ structure. Thus, in the following part we will discuss the representability of these four new problems.

4 Relative representability of level n moduli problems

4.1 The situation in general

Theorem 16. *Let $n \geq 1$ be an integer, and fix an elliptic curve E over a base S. Consider the three functors on $\mathcal{S}\mathrm{ch}_{/S}$ induced by $\Gamma(n)$, $\Gamma_1(n)$ and $\mathrm{Bal}\,\Gamma_1(n)$. Each of these functors is represented by a finite $S-$scheme.*

Proof. This result follows from the following lemma which we do not prove.

Lemma 17. *(See [5, Lemma* 1.3.4 *and Corollary* 1.3.7*]) Let E be a smooth curve over S, let D and D' be two effective Cartier divisors such that D' is proper over the base S. Then:*

1. *There exists a unique closed subscheme $Z \subseteq S$ which is universal for the condition $D = D'$, i.e. such that for all morphisms of schemes $T \longrightarrow S$, then $D_T = D'_T$ if and only if T factors through Z. Z is given locally by* $\deg(D')$ *equations;*
2. *Suppose moreover E is an elliptic curve. Then there exists a unique closed subscheme $Z \subseteq S$ which is universal (in the sense above) for the condition D is a subgroup of E. Z is given locally by* $1+\deg(D')+\deg(D)^2$ *equations.*

In fact, by the previous lemma, it follows that $\Gamma(n)$ is represented by the closed subscheme of $\underline{\mathrm{Hom}}_{S-\mathcal{G}\mathrm{p}}\left((\mathbb{Z}/n\mathbb{Z})^2_S\,,\,E\right)$ over which the effective Cartier divisor $\sum[\Phi(a)]$ in $E\times_S \underline{\mathrm{Hom}}_{S-\mathcal{G}\mathrm{p}}\left((\mathbb{Z}/n\mathbb{Z})^2_S\,,\,E\right)$, given by the universal morphism $\Phi\colon\ (\mathbb{Z}/n\mathbb{Z})^2_S \longrightarrow E[n]$, satisfies $D = E[n]$.
$\Gamma_1(n)$ is represented by the closed subscheme of $\underline{\mathrm{Hom}}_{S-\mathcal{G}\mathrm{p}}\left((\mathbb{Z}/n\mathbb{Z})_S\,,\,E\right) \cong E[n]$ over which the effective Cartier divisor $\sum[\Phi(a)]$ of deg $= n$ in $E\times_S \underline{\mathrm{Hom}}_{S-\mathcal{G}\mathrm{p}}\left((\mathbb{Z}/n\mathbb{Z})_S\,,\,E\right)$, given by the universal morphism $\Phi\colon\ (\mathbb{Z}/n\mathbb{Z})_S \longrightarrow E$, is a subgroup.
Finally, $\mathrm{Bal}\,\Gamma_1(n)$ is represented by the scheme $\mathbb{Z}/n\mathbb{Z}{-}\mathrm{Gen}\left(K'/\left(\Gamma_1(n)(E/S)\right)\right)$, where K' is the tautological quotient of $E[n]$ by the subgroup K specified by a $\Gamma_1(n)-$structure on $[n]$. This scheme is finite over the relative moduli problem $\Gamma_1(n)(E/S)$. ☐

4.2 The situation when n is invertible

Theorem 18. *Let $n \geq 1$ be an integer, let S be a scheme defined over $\mathbb{Z}\left[\frac{1}{n}\right]$, and let E be an elliptic curve over S. Consider the four moduli problems on $\mathcal{S}\mathrm{ch}_{/S}$ induced by $\Gamma(n)$, $\Gamma_1(n)$, $\mathrm{Bal}\,\Gamma_1(n)$ and $\Gamma_0(n)$. Then each one of these functors is representable by a finite and étale $S-$scheme.*

Proof. For the first three functors, the claim follows from the fact that we already know they are finite. Moreover, by Theorem 2, $E[n]$ is finite étale over S and locally isomorphic to the constant group scheme $(\mathbb{Z}/n\mathbb{Z})^2_S$. So one has only to prove that the representatives of these three functors are formally étale: consider a thickening T_0 of T (i.e., a closed subscheme locally given by a nilpotent ideal), and suppose $\Phi_0\colon\ (\mathbb{Z}/n\mathbb{Z})^2_S \longrightarrow E(T_0)$ is a full level n structure (the other cases are analougous). Φ_0 factors through the kernel $E[n](T_0)$ being of degree n. Now $E[n]$ is étale, and in particular formally étale; so there exists a lift $\widetilde{\Phi_0}$ of Φ_0 to $E[n](T)$, and this is a full level n structure on $E(T)$. The proof for $\Gamma_0(n)$ can be found in [5, Theorem 3.7.1]. ☐

In particular, the four moduli problems we have presented here are represented respectively by:

- the constant group scheme

$$S \times \{\mathbb{Z}/n\mathbb{Z} - \text{bases of } (\mathbb{Z}/n\mathbb{Z})^2\}$$

- the constant group scheme

$$S \times \{\text{elements } P \text{ of } (\mathbb{Z}/n\mathbb{Z})^2 \text{ having exact order } n\}$$

- the constant group scheme

$$S \times \left\{ \begin{array}{c} (K,\ P,\ P') \text{ such that } K \text{ is a cyclic subgroup of } (\mathbb{Z}/n\mathbb{Z})^2 \\ \text{of order } n,\ P \text{ is a generator of } K,\ P' \text{ is a generator} \\ \text{of the quotient modulo } K \text{ of } (\mathbb{Z}/n\mathbb{Z})^2 \end{array} \right\}$$

- the constant group scheme

$$S \times \{\text{cyclic subgroups of order } n \text{ in } (\mathbb{Z}/n\mathbb{Z})^2\}$$

Corollary 19. *For $n \geq 3$, the naive level n moduli problem is representable by an affine curve over $\mathbb{Z}\left[\frac{1}{n}\right]$, denoted by $Y(n)$ and called the modular curve.*

Proof. This follows straightforwardly from the previous result on relative representability of naive level n structure and the Proposition 9, using the fact that an automorphism ϕ of a connected elliptic curve E over a base S which induces an identity on $E[n]$ $(n \geq 2)$ can be only $\pm id$ (if $n = 2$) or the identity itself (when $n \geq 3$). $\square$

Remark 20. When S is the spectrum of the field of complex numbers $\mathbb{C}$, then the modular curve $Y(n)$ is just the usual modular curve $Y(n)$ given by the quotient of the upper half plane $\mathbb{H}$ by the action of the subgroup $\Gamma(n)$ of $\mathrm{SL}_2(\mathbb{Z})$ consisting of matrices:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

such that $a \equiv d \equiv \pm 1 \mod n$ and $b \equiv c \equiv 0 \mod n$.

5 Regularity theorem

First of all, let us present an important theorem (which we do not prove).

Theorem 21. *([5, Theorem 5.1]) Let $\mathcal{P}$ be one of the moduli problems $\Gamma(n)$, $\Gamma_1(n)$, $\mathrm{Bal}\,\Gamma_1(n)$, $\Gamma_0(n)$. Then $\mathcal{P}$ is relatively representable over $\mathcal{E}\mathrm{ll}$, is finite and flat over $\mathcal{E}\mathrm{ll}$ of constant rank ≥ 1, and it is regular of dimension 2. Each is finite étale over $\mathcal{E}\mathrm{ll}_{/\mathbb{Z}\left[\frac{1}{n}\right]}$.*

Proof. (Sketch) This theorem is true over $\mathbb{Z}\left[\frac{1}{n}\right]$, and by 15 we can reduce ourselves to the case when n is the power of a single prime p. Then one proves using the homogeneity principle ([1]) that the statement holds for all moduli problems $\mathcal{P}$ such that, fixing a prime $p \neq 0$:

1. $\mathcal{P}$ is relatively representable;
2. $\mathcal{P} \otimes \mathbb{Z}\left[\frac{1}{n}\right]$ is finite étale;
3. For all E, E' elliptic curves over S, for any isomorphisms ϕ between $p-$divisible subgroups $E[p^\infty] \xrightarrow{\cong} E'[p^\infty]$ then $\mathcal{P}(\phi)$ is an isomorphism between $\mathcal{P}_{E'/S}$ and $\mathcal{P}_{E/S}$;
4. Let k an algebraically closed field over $\mathbb{F}_p$. Let E_0 be a supersingular elliptic curve over k and consider $\mathbb{E}$ be the universal formal deformations over the formal power series with coefficients in the Witt vector ring $W(k)[\![t]\!]$. Then $\mathcal{P}(E_0/k) \cong \{*\}$ and $\mathcal{P}_{\mathbb{E}/W(k)[\![t]\!]}$ is the spectrum of a regular $2-$dimensional local ring.

□

Now we can state our main result on the regularity of our moduli problems (we repeat some facts we have already seen to give the whole picture).

Theorem 22. *Let $n \geq 1$ be an integer. Consider $\mathcal{S}$ a representable moduli problem which is étale over $\mathcal{E}\mathrm{ll}$, and let $\mathcal{P}$ be one of the moduli problems $\Gamma(n)$, $\Gamma_1(n)$, $\mathrm{Bal}\,\Gamma_1(n)$, $\Gamma_0(n)$. Then:*

1. *$\mathscr{M}(\mathcal{S},\,\mathcal{P})$ is a regular $2-$dimensional scheme, finite and flat over $\mathscr{M}(\mathcal{S})$;*
2. *$\mathscr{M}(\mathcal{S},\,\mathcal{P}) \otimes \mathbb{Z}\left[\frac{1}{n}\right]$ is finite étale over $\mathscr{M}(\mathcal{S},\,\mathcal{P}) \otimes \mathbb{Z}\left[\frac{1}{n}\right]$;*
3. *$\mathscr{M}(\mathcal{S},\,\mathcal{P})$ is flat over $\mathbb{Z}$;*
4. *$\mathscr{M}(\mathcal{S},\,\mathcal{P})$ is the normalization of $\mathscr{M}(\mathcal{S})$ in $\mathscr{M}(\mathcal{S},\,\mathcal{P}) \otimes \mathbb{Z}\left[\frac{1}{n}\right]$;*

Proof. The first two statements were already stated (they are respectively the statement of the previous theorem, and Theorem 18). The third follows from the first together with the fact that $\mathcal{S}$ is flat over $\mathbb{Z}$, and finally the fourth follows from the first two because the normalization is the unique normal scheme finite over $\mathscr{S}$ and it agrees, over $\mathbb{Z}\left[\frac{1}{n}\right]$, with $\mathscr{M}(\mathcal{S},\,\mathcal{P})$. □

6 Coverings of the moduli spaces

Theorem 23. *Let $n \geq 1$ be an integer, let E be an elliptic curve over S. Consider two $S-$points P and Q in $E[n](S)$ which are a Drinfeld $n-$basis of E over S. Then:*

1. *P is a $\Gamma_1(n)-$structure on E over S;*
2. *Let K be the cyclic subgroup of $E[n]$ generated by P. Given $[Q]$ the image of Q via the quotient morphism $E \longrightarrow E'$ (where $E' = E/K$) then $[Q]$ is a $\Gamma_1(n)-$structure on E'. In particular, it generates $K' := E[n]/K$ and thus the triple $(P,\ K,\ Q)$ is a balanced $\Gamma_1(n)-$structure.*

Proof. The theorem is obvious when n is invertible on S. The question is f.p.p.f. local over the base, so we can assume ℓ is an odd prime which is invertible on S and such that E admits a naive full level ℓ structure (whose associated moduli problem $\mathcal{S}$ is representable, by Theorem 19). So we reduce to the universal base: assume S is $\mathscr{M}(\mathcal{S},\ \Gamma(n))$ and let $\mathbb{E}$ be the universal elliptic curve defined over it with a universal $\Gamma(n)-$structure. In particular S is flat over $\mathbb{Z}$ and affine (say $S = \operatorname{Spec}(A)$).

1. Recall that $\Gamma_1(n)$ is representable bu a closed subscheme $\mathcal{P}_{\mathbb{E}/S}$ of $\mathbb{E}[n] = \underline{\operatorname{Hom}}\left((\mathbb{Z}/n\mathbb{Z})_S,\ \mathbb{E}\right)$. Let $I = (f_1, \ldots,\ f_r)$ be the ideal defining $\mathcal{P}_{E/S}$: then $f_i(P) = 0$ in $A\left[\frac{1}{n}\right]$ and since A is flat over $\mathbb{Z}$ we have an inclusion $A \hookrightarrow A\left[\frac{1}{n}\right]$ which yields that $f_i(P) = 0$ also in A.
2. Since the scheme of generators of K' is a closed subscheme of $K' \cong \underline{\operatorname{Hom}}\left((\mathbb{Z}/n\mathbb{Z})_S,\ K'\right)$ we can conclude as in 1..

☐

Corollary 24. *The previous theorem yields natural morphisms of moduli problems:*

$$\Gamma(n) \overset{\deg = n}{\longrightarrow} \operatorname{Bal}\Gamma_1(n) \overset{\deg = \phi(n)}{\longrightarrow} \Gamma_1(n)$$

which are finite and flat of indicated degrees. In other words: for every representable moduli problem $\mathcal{S}$ we have a natural diagram of morphisms, each of which is flat of indicated degree:

$$\begin{tikzcd}
\mathscr{M}(\mathcal{S},\ \Gamma(n)) \arrow[d, "\deg = n"] \arrow[ddd, bend right=60, "\deg = \#\,\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})"'] \\
\mathscr{M}(\mathcal{S},\ \operatorname{Bal}\Gamma_1(n)) \arrow[d, "\deg = \phi(n)"] \\
\mathscr{M}(\mathcal{S},\ \Gamma_1(n)) \arrow[d, "\deg = n^2 \cdot \prod_{p|n}\left(1 - \frac{1}{p^2}\right)"] \\
\mathscr{M}(\mathcal{S})
\end{tikzcd}$$

Proof. The existence of these morphisms is precisely the statement of the previous theorem. To prove they are finite and flat of asserted degrees, we reduce to the case when $\mathcal{S}$ is étale over $\mathcal{E}\mathrm{ll}$ and $\mathscr{M}(\mathcal{S})$ is connected. In this case all the schemes involved are regular 2−dimensional schemes finite over $\mathscr{M}(\mathcal{S})$ (this is the statement of Theorem 22), and thus the morphisms are necessarily all finite and flat. To compute the degrees, since $\mathscr{M}(\mathcal{S})$ is flat over $\mathbb{Z}$ we may invert n and then the result is a trivial consequence of Section 4.2 and of the description we gave of the representatives of these moduli problems. $\square$

References

[1] P. Deligne and M. Rapoport. Les schémas de modules de courbes elliptiques. pages 143–316. Lecture Notes in Math., Vol. 349, 1973.

[2] V. G. Drinfeld. Elliptic modules. *Mat. Sb. (N.S.)*, 94(136):594–627, 656, 1974.

[3] Alexander Grothendieck, Michèle Raynaud, Michel Demazure, Michael Artin, Jean-Louis Verdier, Pierre Deligne, Pierre Berthelot, Luc Illusie, and Nicholas Katz. *Séminaire de Géométrie Algébrique du Bois-Marie.* Springer-Verlag, Berlin, 1970-1973. Lecture Notes in Mathematics, Vols. 151, 152, 153, 224, 225, 269, 270, 288, 305, 340, 569, and 589.

[4] Jun-ichi Igusa. Fibre systems of Jacobian varieties. III. Fibre systems of elliptic curves. *Amer. J. Math.*, 81:453–476, 1959. ISSN 0002-9327. doi: 10.2307/2372751. URL `https://doi.org/10.2307/2372751`.

[5] Nicholas M. Katz and Barry Mazur. *Arithmetic moduli of elliptic curves*, volume 108 of *Annals of Mathematics Studies.* Princeton University Press, Princeton, NJ, 1985. ISBN 0-691-08349-5; 0-691-08352-5. doi: 10.1515/9781400881710. URL `https://doi.org/10.1515/9781400881710`.