Next step: Extend the previous constructions to

- allow other kinds of level structure ("$\Gamma(N)$, $\Gamma_1(N)$, ...", see below)
- remove the condition that one of 2, 3 is invertible.

To do so, we will start with $\mathcal{M}_{\text{Legendre}}$ and $\mathcal{M}_3$ as above and study moduli functors defined by adding further additional data ("level structure") to define relatively representable functors in the following sense:

Def Let S be a scheme. A morphism $F \to G$ of functors $(\mathrm{Sch}/S)^{op} \to (\mathrm{Sets})$ is called (relatively) representable if for all S-schemes X and morphisms $X \to G$ the fiber product functor $F \times_G X : T \mapsto F(T) \times_{G(T)} X(T)$ is representable by an S-scheme.

In the situation of the above definition we say that a representable $F \to G$ has a certain property P of scheme morphisms (e.g., finite, étale, ...), if for every $X \to G$ the scheme morphism $F \times_G X \to X$ has the property P.

Denote by $\mathcal{M}: (\mathrm{Sch})^{op} \to (\mathrm{Sets})$ the functor

$$S \mapsto \{E/S \text{ elliptic curve}\}/\cong$$

($\mathcal{M}$ is <u>not</u> representable, see the above discussion).

Let S be a scheme, E/S an elliptic curve.

A level-N-structure (or a level structure of type $\Gamma(N)$) on E/S is an isomorphism $\alpha: (\underline{\mathbb{Z}/N})^2 \xrightarrow{\sim} E[N]$.

(This can exist only if $N \in \mathcal{O}_S^\times$.)

Let $\mathcal{M}_N: (\mathrm{Sch}/\mathbb{Z}[\tfrac{1}{N}])^{op} \longrightarrow (\mathrm{Sets})$

$$S \longmapsto \left\{ (E,\alpha);\ \begin{array}{l} E/S \text{ elliptic curve}, \\ \alpha: (\underline{\mathbb{Z}/N})^2 \xrightarrow{\sim} E[N] \\ \text{level-}N\text{-structure} \end{array} \right\} \Big/ \cong$$

Other interesting types of level structure one could consider are

- $\Gamma_1(N)$ (N invertible on S)

  $P \in E[N](S)$ of exact order N (i.e. dP disjoint from 0 for all $d \mid N$, $1 \le d < N$)

  (i.e. dP disjoint from 0

  can test this after finite étale base change $S' \to S$ (and WLOG $E[N]$ constant)

- $\Gamma_0(N)$ (N arbitrary)

  $H \subseteq E[N]$ $\underbrace{\text{cyclic}}$ subgroup scheme of order N

  automatic if N is a prime number

Theorem (relative representability).

Let S be a scheme $/\mathbb{Z}[\frac{1}{N}]$, E/S an elliptic curve.

(1) The functor $(Sch/S)^{op} \to (Sets)$

$$T \mapsto \{\Gamma(N)\text{-structures on } E_T/T\}$$

is representable by a finite étale S-scheme.

(1') The forgetful morphism $\mathcal{M}_N \to \mathcal{M}$ is repres.,

$$(E,\alpha) \mapsto E$$

finite, étale.

(2) The functor $(Sch/S)^{op} \to (Sets)$

$$T \mapsto \{\Gamma_1(N)\text{-str. } P \text{ on } E_T/T\}$$

is repres. by a finite étale S-scheme.

(2') The forgetful morphism $\mathcal{M}_{\Gamma_1(N)} \to \mathcal{M}$

$$(E,P) \mapsto E$$

is representable, finite étale.

Proof The equivalences $(1) \Leftrightarrow (1')$, $(2) \Leftrightarrow (2')$ hold for purely formal reasons:

Namely, by definition, $\mathcal{M}_N \to \mathcal{M}$ repres.

$\iff \forall\ S \to \mathcal{M}$: $\quad \mathcal{M}_N \times_{\mathcal{M}} S : \left(Sch/\mathbb{Z}[\tfrac{1}{N}]\right)^{op} \to (Sets)$ repr.

$\iff \forall\ S \to \mathcal{M}$: $\quad \mathcal{M}_N \times_{\mathcal{M}} S : (Sch/S)^{op} \to (Sets)$

$$\begin{array}{c} T \\ f\downarrow \\ S \end{array} \longmapsto \mathcal{M}_N(T) \times_{\mathcal{M}(T)} \underbrace{S(T)}_{=\{f\}}$$

consider S-morphisms

$$\begin{tikzcd} T \arrow[r] \arrow[dr, "f"'] & S \arrow[d, "id"] \\ & S \end{tikzcd}$$

is repres. by an S-scheme M

(i.e. $\quad$ $\begin{tikzcd} \mathcal{M}_N \times_{\mathcal{M}} S \arrow[r, "\sim"] \arrow[d, "pr"'] \arrow[dr, phantom, "\circlearrowleft"] & M \arrow[d] \\ S \arrow[r, "id"] & S \end{tikzcd}$)

$\operatorname{Spec} \mathbb{Z}[\tfrac{1}{N}]$ in our case

Lemma S_0 a scheme, S an S_0-scheme, $F \to S$ a morphism of functors $(Sch/S_0)^{op} \to (Sets)$.

Then F is repres. by a scheme M

$\iff$ $\quad F|_{(Sch/S)^{op}}$ is repres. by an S-scheme M s.t. the diagram $\begin{tikzcd} F \arrow[rr, "\cong"] \arrow[dr] & & M \arrow[dl] \\ & S & \end{tikzcd}$ commutes.

Proof '$\Rightarrow$' Define $M \to S$ as the composition $M \cong F \to S$.

'$\Leftarrow$' Let T be any scheme. For $a: T \to S$ write T_a for the S-scheme $\begin{array}{c} T \\ \downarrow a \\ S \end{array}$

$$F(T) = \dot{\bigcup_{a \in S(T)}} F_S(T_a) = \dot{\bigcup_{a}} M_S(T_a) = M(T) \qquad (-_S(\,)\text{ means } S\text{-morph.})$$

Now let us prove (1).

First note that the functor

$$T \longmapsto \{P \in E[N](T)\}$$

is trivially representable by $E[N]$.

Giving a group scheme homomorphism $(\underline{\mathbb{Z}/N})^2 \longrightarrow E[N]$ is the same as specifying two points $P, Q \in E[N](T)$, so $\mathrm{Hom}((\underline{\mathbb{Z}/N})^2, E[N])$ is repres. by $E[N] \times_S E[N]$.

This is finite étale $/S$, so it is enough to show that the subfunctor $\mathrm{Isom}((\mathbb{Z}/N)^2, E[N])$ of isomorphisms $(\underline{\mathbb{Z}/N})^2 \cong E[N]$ is repres. by an open and closed subscheme of $\mathrm{Hom}((\underline{\mathbb{Z}/N})^2, E[N]) = E[N] \underset{S}{\times} E[N]$.

The condition when P, Q give rise to a point on $\mathrm{Isom}((\underline{\mathbb{Z}/N})^2, E[N])$ is that for all $a, b \in \mathbb{Z}/N$, $\begin{pmatrix} a \\ b \end{pmatrix} \neq \begin{pmatrix} 0 \\ 0 \end{pmatrix}$, $aP + bQ$ disjt from 0.

Let $K_{a,b} := \mathrm{Ker}\Big(E[N]^2 \xrightarrow{\begin{pmatrix} a \\ b \end{pmatrix}} E[N] \Big).$

$$(P_1, P_2) \longmapsto aP_1 + bP_2$$

Then $K_{a,b}$ is finite étale $/S$ (since the morphism $\begin{pmatrix} a \\ b \end{pmatrix}$ is finite étale, both source and target being finite étale $/S$), thus $K_{a,b} \subseteq E[N]^2$ open + closed.

Thus $\mathrm{Isom}((\underline{\mathbb{Z}/N})^2, E[N]) = E[N]^2 \setminus \bigcup_{\begin{pmatrix} a \\ b \end{pmatrix} \neq \begin{pmatrix} 0 \\ 0 \end{pmatrix}} K_{a,b}$

is open and closed $\subset E[N]$ and in particular finite étale $/S$.

(2) Saying that $P \in E[N](T)$ has exact order N means that

$$P \in \underbrace{\Big(E[N] \setminus \bigcup_{\substack{d \mid N \\ 1 \le d < N}} E[d]\Big)}_{\subset E[N] \ \boxed{\text{open and closed}} \ \rightsquigarrow \ \text{finite étale}/S}(T)$$

$$E[d] = \mathrm{Ker}\big(E[N] \xrightarrow{d} E[N]\big) \longrightarrow E[N]$$

open + closed (source + target are finite étale, hence so is the map)

so this functor is representable by $E[N] \setminus \bigcup E[d]$.

Plan for showing that $\mathcal{M}_N$ (ell. c. + level-N-str.) is representable $/ \mathbb{Z}[\frac{1}{N}]$.

(1) By gluing, enough to show that both restrictions to $(\mathrm{Sch}/\mathbb{Z}[\frac{1}{2N}])^{op}$ and $(\mathrm{Sch}/\mathbb{Z}[\frac{1}{3N}])^{op}$ are representable.

(2) $/\mathbb{Z}[\frac{1}{3N}]$ Let $\mathcal{M}_{N,3} = \mathcal{M}_N \times_{\mathcal{M}} \mathcal{M}_3$

$$\left(S \mapsto \left\{\left(E/S,\ \alpha: (\mathbb{Z}/N)^2 \to E[N],\ \beta: (\mathbb{Z}/3)^2 \to E[3]\right)\right\}_{/\cong}\right)$$

Since $\mathcal{M}_3$ is repres. and $\mathcal{M}_N \to \mathcal{M}$ is rel. repr., $\mathcal{M}_{N,3}$ is repres (by a smooth affine $\mathbb{Z}[\frac{1}{3N}]$-scheme of relative dim. 1). The fibers of the forgetful map $\mathcal{M}_{N,3} \to \mathcal{M}_N$ are (empty or) in bijection with $GL_2(\mathbb{Z}/3)$ (see the notion of $GL_2(\mathbb{Z}/3)$-torsor below), so $\mathcal{M}_N$ "looks like a quotient of $\mathcal{M}_{N,3}$ by the $GL_2(\mathbb{Z}/3)$-action $g \cdot (E/S, \alpha, \beta) := (E/S, \alpha, \beta \circ g)$.
We will construct the scheme quotient $\mathcal{M}_{N,3}/GL_2(\mathbb{Z}/3)$ and show it represents $\mathcal{M}_N$.

$$\begin{tikzcd}[column sep=small] & GL_2(\mathbb{Z}/3) \curvearrowright \mathcal{M}_{N,3} \arrow[dl] \arrow[dr] & \\ \mathcal{M}_{N,3}/GL_2(\mathbb{Z}/3) \arrow[rr, dashed, "\sim"] & & \mathcal{M}_N \end{tikzcd}$$

Torsors

S scheme, G/S a group scheme

X, Y schemes $/S$, $G \times_S X \xrightarrow{\rho} X$ group scheme action,

$X \xrightarrow{f} Y$ a G-invariant morphism ("$f(gx) = f(x)$ $\forall g \in G, x \in X$"

$\Updownarrow$

$$\begin{tikzcd} G \times X \arrow[r, "\rho"] \arrow[d, "pr_2"'] \arrow[dr, phantom, "\circlearrowleft"] & X \arrow[d] \\ X \arrow[r] & Y \end{tikzcd}$$)

We say that f is a <u>G-torsor</u> (or a principal homogeneous space under G)

if (1) $G \times_S X \xrightarrow{\sim} X \times_Y X$

$(g, x) \longmapsto (x, gx)$

is an isomorphism

(2) there exists a "covering" $Y' \to Y$

and a section s of $Y' \times_Y X \xrightarrow{pr} Y'$

i.e. $pr \circ s = id_{Y'}$

Note: The notion of torsor depends on specifying what is meant by "covering", see below.

Explanation.

- Consider $T \xrightarrow{y} Y$ then
$$\begin{tikzcd} T \arrow[r] \arrow[dr] & X \times_Y X \arrow[d] \\ & Y \end{tikzcd}$$
is the same as a pair $T \underset{x'}{\overset{x}{\rightrightarrows}} X$ of lifts of $T \to Y$.

So (1) says that for any pair x, x' of lifts of y, there exists a unique $g \in G(T)$ s.t. $gx = x'$.

In other words: for all Y-schemes T, $G(T)$ acts simply transitively on $\mathrm{Hom}_Y(T, X)$ (this set could be empty).

- "Locally" on Y, i.e., after pulling back to a covering Y' as in (2), all fibers of $X \to Y$ are non-empty; enough to check the universal fiber

$$\begin{array}{ccc} s & \longmapsto & \mathrm{id} \\ \cap & & \cap \\ (Y' \times X)(Y') & \longrightarrow & Y'(Y') \end{array}$$

Standard types of coverings one could consider (among several others...)

- Zariski, i.e. $Y' = \coprod U_i \to Y$ where $Y = \bigcup_{i \in I} U_i$ is a covering by open subschemes

- fppf (fidèlement plat + présentation finie = faithfully flat, finite presentation):

  $Y' \to Y$ is a flat morphism locally of finite presentation. (Recall that such morphisms are open.)

  (This is much more general than Zariski covering. In the literature, by 'torsor' (without further specification) one usually means 'torsor w.r.t. fppf covers'.)

- étale, $Y' \to Y$ is an étale morphism

  (This is in between:

  $$\text{Zariski cover} \Rightarrow \text{étale} \Rightarrow \text{fppf}.)$$

This is the notion we will use in the sequel (and typically finite étale $Y' \to Y$ will suffice for us).

Examples (1) Let S be a scheme $/ \mathbb{Z}[\frac{1}{N}]$, $N \geq 1$,
E/S an elliptic curve.

Then $\mathrm{Isom}\left((\underline{\mathbb{Z}/N})^2, E[N]\right)$ is representable (see above)

and $\mathrm{Isom}\left((\mathbb{Z}/N)^2, E[N]\right) \to S$ is a $\underline{GL_2(\mathbb{Z}/3)}$-torsor.

(2) Let $X \xrightarrow{f} Y$ be an isogeny of abelian varieties
(over some scheme S) with kernel K.

Then $K \times_S X \cong X \times_Y X$ $\quad \left(K \times_S X = X \times_{Y,e} S \times_S X \right.$
$\left. \cong X \times_Y X \right)$.

Since $X \times_Y X \to X$ trivially
has a section (the diagonal),
we see that f is a K-torsor for any notion
of covering s.t. f is a covering.

Since isogenies are flat + locally of finite pres.,
every isogeny is an fppf-torsor.

If f étale ($\Longleftrightarrow$ K étale$/S$) then f is a torsor
w.r.t. étale coverings.

'$\Leftarrow$' Can check whether f étale
after faithfully flat base
change and $X \times_Y X \cong K \times_S X$

$$\begin{tikzcd}[column sep=small] X \times_Y X \arrow[dr] & \cong & K \times_S X \arrow[dl] \\ & X & \end{tikzcd}$$

Remark If K is not étale, then f cannot acquire a section after an étale base change $Y' \to Y$. In fact, if $X \times Y' \to Y'$ has a section, then $X \times_S Y' \cong K \times_S Y'$ (as Y'-schemes, see the discussion of the trivial torsor below).

$$\rightsquigarrow \quad K \times_S Y' \xrightarrow{\sim} X \times_Y Y' \xrightarrow{\text{étale if } Y'/Y \text{ étale}} X \xrightarrow{\text{smooth}} S, \quad \text{i.e.}$$

$K \times_S Y'$ smooth $/S$. But then K is smooth$/S$ (hence étale, for dimension reasons), since Y'/S faithfully flat.

Example (3) L/K a finite Galois extension with Galois group G. Then $\operatorname{Spec} L \to \operatorname{Spec} K$ is a G-torsor (for étale coverings, in fact $\operatorname{Spec} L \to \operatorname{Spec} K$ "trivializes" this torsor).

- Trivial torsor: $X = G\times_S Y$ equivariant w.r.t. action on RHS by (left) multiplication
$$\begin{array}{c} X = G\times_S Y \\ \downarrow \\ Y \end{array}$$

<u>Lemma</u> (1) Let $X \to Y$ be a G-torsor. Then $X\to Y$ is isomorphic to the trivial torsor if and only if $X \to Y$ has a section.

(2) Let $X\to Y$, $X'\to Y$ be G-torsors and let $X \xrightarrow{g} X'$ be a G-equivariant morphism of Y-schemes. Then g is an isomorphism.

Proof (1) Clearly the trivial torsor has a section (the neutral element of G).

Conversely, suppose that $X\to Y$ has a section s.

We define $\quad G\times_S Y \to X, \quad g \mapsto gs,$

(as usual, to be read on T-valued pts for Y-schemes T: $\begin{array}{c} T \\ \downarrow a \\ Y\end{array}$

s defines $s_T : T \to X$ by composition $T \xrightarrow{a} Y \xrightarrow{s} X$

and $(G\times_S Y)(T) \circlearrowright X(T)$, so $g\cdot s_T$ "makes sense".)

By the definition of "torsor", $(G\times_S Y)(T) \circlearrowright X(T)$ morph. $T\to X$ of Y-sch.

simply transitively, so the map is bijective.

(2) We can check whether $X \to X'$ is an isom. after any faithfully flat base change, i.e., if $Y' \to Y$ fppf and $X \times_Y Y' \to X' \times_Y Y'$ is an isomorphism then $X \to X'$ is an isom. (cf. e.g. [GW1] Prop. 14.53).

Thus we may assume that both X and X' are trivial torsors. In this case the claim follows immediately since the morphism is G-equivariant.

Existence of quotients

References

Mumford, Abelian varieties, §12, see also §7,

Edixhoven, van der Geer, Moonen, Abelian varieties

Stix, Finite flat gp sch.

SGA III, Demazure-Gabriel

Theorem Let S be a scheme,

G/S a finite locally free gp scheme,

X a separated S-scheme

equipped with a G-action $G \times_S X \to X$.

Assume that X can be covered by G-stable affine open subschemes.

Y/S separated ✓

Then there exists a morphism $\pi : X \to Y$,

s.t. (1) As a topol. space, Y is the quotient of the topol space X by

$P \sim Q \iff \exists R \in G \times_S X : pr_X(R) = P, \ \varrho(R) = Q$,

and $\mathcal{O}_Y = (\pi_* \mathcal{O}_X)^G \hookrightarrow \pi_* \mathcal{O}_X$

$f \in (\pi_* \mathcal{O}_X)^G :\iff pr_X^*(f) = \varrho^*(f)$

[We can phrase this by saying that Y is the coequalizer of $G \times X \overset{\rho}{\underset{pr_X}{\rightrightarrows}} X$ in (Ringed Sp.)

NB: One sometimes says that "Y is the quotient of X by G in the cat. of ringed spaces", but G may not be a group object in this category (since the products in (Sch) and (RS) usually differ).]

(2) π satisfies the universal property of the quotient of X by G:

$$\begin{tikzcd} X \arrow[r] \arrow[d] & Z \\ Y \arrow[ur, dashed, "\exists!"'] & \end{tikzcd}$$ G-invar. morph.

(3) π is quasi-finite, integral and surjective.

If S locally noetherian and X/S of finite type, then π is finite and Y/S of finite type.

(4) The formation of the quotient is compatible with flat base change $S' \to S$.

(5) If the G-action on X is (strictly) free (by definition this means that the natural map

$$G \times_S X \to X \times_S X \quad \text{is a closed immersion})$$

then π is finite locally free and

$$G \times_S X \xrightarrow{\sim} X \times_Y X \quad \text{is an isomorphism}$$

Moreover, in this situation the construction of the quotient commutes with arbitrary base change.

We call Y the quotient of X by G and write $G\backslash X := Y$. (or similarly X/G in case of right action).

$\boxed{9.7.2024}$

<u>Remark</u> (Relation to torsors) In the situation of (5) (i.e., when $G \circlearrowright X$ free), then X is a G-torsor whenever $G \to S$ is a covering morphism

($G \to S$ covering $\rightsquigarrow$ $X \times_Y X \cong G \times_S X \to X$ covering
$\underset{\pi \text{ fppf}}{\rightsquigarrow}$ $X \to Y$ covering, and $X \times_Y X \to X$ has section).

Cor Let S be a scheme, G/S finite loc. free, X, Y sep./S, $X \to Y$ a G-torsor. Then there exists a unique isomorphism ${}_G\backslash X \xrightarrow{\sim} Y$ s.t.

$$\begin{tikzcd} & X \arrow[dl] \arrow[dr] & \\ {}_G\backslash X \arrow[rr, "\sim"] & & Y \end{tikzcd}$$

commutes.

(Note that for $X \to Y$ a G-torsor, X, Y separated/S, the G-action is necessarily free: $G \times_S X \underset{\substack{\uparrow \\ \text{by defn of torsor}}}{\xrightarrow{\sim}} X \times_Y X \to X \times_S X$ closed imm.: $\begin{tikzcd} X \times_Y X \arrow[r] \arrow[d] \arrow[dr, phantom, "\square"] & X \times_S X \arrow[d] \\ Y \arrow[r, "\Delta"] & Y \times_S Y \end{tikzcd}$)

Proof. The uniqueness is clear since $X \to {}_G\backslash X$, $X \to Y$ are epimorphisms.

By the universal property of the quotient, we obtain a morphism ${}_G\backslash X \to Y$ s.t.

$$\begin{tikzcd} & X \arrow[dl] \arrow[dr] & \\ {}_G\backslash X \arrow[rr, "\sim"] & & Y \end{tikzcd}$$

commutative.

We may check that ${}_G\backslash X \to Y$ is an isomorphism after base change with an fppf morphism $Y' \to Y$.

This means that we may assume that X is the trivial G-torsor i.e. $X \cong G \times_S Y$ (G-equivariantly). But then ${}_G\backslash X \cong Y$, as desired.

Proof of theorem (quotients by finite loc.-free grp sch.)

(sketch / some remarks)

- reduce to S (hence G) affine (easy)

  and to X affine (easy using the assumption that X has cover by G-stable affine opens;

  NB There exist examples of $G \circlearrowright X \to S$ where this is not satisfied and hence a quotient cannot exist!)

So say $S = \operatorname{Spec} R$, $X = \operatorname{Spec} A$, $G = \operatorname{Spec} \Gamma$.

From $G \times_S X \overset{\rho}{\underset{pr}{\rightrightarrows}} X$ get $A \overset{\rho^a}{\underset{pr^a}{\rightrightarrows}} \Gamma \otimes_R A$,

and we let $A^G := \{ s \in A ; \ \rho^a(s) = pr^a(s) \ (= 1 \otimes s) \}$

be the subring of "invariants under the G-action" on A. Evaluating the universal property of the quotient on affine test schemes shows that (if a quotient $G \backslash X$ exists) $G \backslash X = \operatorname{Spec} A^G$.

To go on, assume for simplicity that G is a constant gp scheme, corresp. to some abstract gp which we denote by G as well.

- $|\operatorname{Spec} A^G| = {}_G\backslash|\operatorname{Spec} A|$:

  Define $N: A \to A^G$, $a \mapsto \prod_{g\in G} g(a)$.

  Let $\mathfrak{p}, \mathfrak{p}' \in \operatorname{Spec} A$. If there ex. $g \in G$ with $\mathfrak{p}' = g(\mathfrak{p})$, then $\mathfrak{p} \cap A^G = \mathfrak{p}' \cap A^G$. Conversely, if $\mathfrak{p} \cap A^G = \mathfrak{p}' \cap A^G$, then $N(\mathfrak{p}) \subseteq \mathfrak{p}' \underset{\mathfrak{p}' \text{ prime}}{\leadsto} \mathfrak{p} \subset \bigcup_g g(\mathfrak{p}') \underset{\substack{\text{prime}\\\text{avoidance}}}{\leadsto} \underset{\text{some } g}{\mathfrak{p} \subseteq g(\mathfrak{p}')}$,

  By symmetry, $\mathfrak{p}' \subseteq h(\mathfrak{p}) \subseteq hg(\mathfrak{p}') \subseteq (hg)^2(\mathfrak{p}') \underset{G \text{ finite}}{\subseteq \dots} \subseteq \mathfrak{p}'$

  $\leadsto$ $\mathfrak{p}, \mathfrak{p}'$ in same G-orbit.

- $A^G \to A$ integral: $a \in A$ is a zero of the monic polynomial $\prod_{g\in G}(T - g(a)) \in A^G[T]$.

Representability: level $\Gamma(N)$ over $\mathbb{Z}[\frac{1}{N}]$

Let $N \geq 3$.

The functor $\mathcal{M}_N : (Sch/\mathbb{Z}[\frac{1}{N}])^{op} \to (Sets)$

$$S \mapsto \{(E/S \text{ elliptic curve}, \alpha : (\underline{\mathbb{Z}/N})^2 \xrightarrow{\sim} E[N] \text{ iso})\}/\cong$$

is repres. by an affine $\mathbb{Z}[\frac{1}{N}]$-scheme, smooth of relative dimension 1.

Proof. As explained above, by gluing it is enough to show that the restrictions of $\mathcal{M}_N$ to $(Sch/\mathbb{Z}[\frac{1}{3N}])^{op}$ and to $(Sch/\mathbb{Z}[\frac{1}{2N}])^{op}$ are representable (by affine smooth curves).

We explain the case of $\mathbb{Z}[\frac{1}{3N}]$. The other case is similar (replace $\mathcal{M}_3$ and $GL_2(\mathbb{Z}/3)$ by $\mathcal{M}_{Legendre}$ and $GL_2(\mathbb{Z}/2) \times \mathbb{Z}/2$, or by $\mathcal{M}_4$ (after showing its representability directly) and $GL_2(\mathbb{Z}/4)$).

We have shown that $\mathcal{M}_3$ is repres. and that $\mathcal{M}_N \to \mathcal{M}$ is rel. representable, so

$$\mathcal{M}_{N,3} := \mathcal{M}_N \times_{\mathcal{M}} \mathcal{M}_3 : (\mathrm{Sch}/\mathbb{Z}[\tfrac{1}{3N}])^{op} \to (\mathrm{Sets})$$

$$S \longmapsto \left\{ \left(E/S \text{ ell-c.}, \alpha : (\mathbb{Z}/N)^2 \xrightarrow{\sim} E[N], \beta : (\mathbb{Z}/3)^2 \xrightarrow{\sim} E[3] \right) \right\} /_{\cong}$$

is repres. (by an affine smooth relative curve $/\mathbb{Z}[\tfrac{1}{3N}]$).

The group $G := GL_2(\mathbb{Z}/3)$ (viewed as constant gp scheme) acts on $\mathcal{M}_{N,3}$ by $g \cdot (E, \alpha, \beta) := (E, \alpha, \beta g)$.

<u>Claim</u> The action of G on $\mathcal{M}_{N,3}$ is strictly free.

<u>Proof of claim</u> Need to show: the morphism

$$G \times_{\mathbb{Z}[\frac{1}{3N}]} \mathcal{M}_{N,3} \longrightarrow \mathcal{M}_{N,3} \times_{\mathbb{Z}[\frac{1}{3N}]} \mathcal{M}_{N,3}$$

is a closed immersion.

Clearly it is a monomorphism (injective on S-valued points for every S).

Further, $G \times_{\mathbb{Z}[\frac{1}{3N}]} \mathcal{M}_{N,3} = \coprod_{g \in GL_2(\mathbb{Z}/3)} \mathcal{M}_{N,3}$

and for fixed g the map

$$\begin{array}{ccc} \mathcal{M}_{N,3} & \longrightarrow & \mathcal{M}_{N,3} \times \mathcal{M}_{N,3} \\ x & \longmapsto & (x, gx) \end{array}$$ has a retraction (pr_1)

and hence, being separated, is a closed immersion.

This implies the claim. $\lrcorner$

Thus the quotient $\mathcal{M}_{N,3} \to \mathcal{M}_{N,3}/G$ exists and is a G-torsor.

<u>Claim</u> There exists a (unique) isom. $\mathcal{M}_{N,3}/G \xrightarrow{\sim} \mathcal{M}_N$ of functors $(\mathrm{Sch}/\mathbb{Z}[\frac{1}{3N}])^{op} \to (\mathrm{Sets})$ s.t.

$$\begin{tikzcd} & \mathcal{M}_{N,3} \arrow[dl] \arrow[dr] & \\ \mathcal{M}_{N,3}/G \arrow[rr, "\sim"] & & \mathcal{M}_N \end{tikzcd}$$ commutes.

<u>Remark</u>: If $\mathcal{M}_N$ is representable, then $\mathcal{M}_{N,3} \to \mathcal{M}_N$ is a G-torsor and thus the claim must be true. $\lrcorner$

Proof of claim $\boxed{10.7.2024}$

Step ① Construct morphism $\mathcal{M}_{N,3}/G \to \mathcal{M}_N$.

In other words, we need to find an elliptic curve over $\mathcal{M}_{N,3}/G$ together with a level-N structure.

[This is usually, e.g., in [Katz-Mazur] formulated as a "descent problem". Since we did not study descent so far, we will phrase the situation slightly differently and use the existence of quotients once more.]

Let $(E^{univ}, \alpha^{univ}, \beta^{univ})$ be the universal object over $\mathcal{M}_{N,3}$. For $g \in G$, $(E^{univ}, \alpha^{univ}, \beta^{univ} g)$

defines $g : \mathcal{M}_{N,3} \to \mathcal{M}_{N,3}$ the unique morphism with $g^*(E^{univ}, \alpha^{univ}, \beta^{univ}) \cong (E^{univ}, \alpha^{univ}, \beta^{univ} g)$.

In particular, forgetting the third component, we obtain automorphism

$$\underbrace{g^*(E^{univ}, \alpha^{univ})}_{\substack{\parallel \\ \left(E^{univ} \times_{\mathcal{M}_{N,3}, g} \mathcal{M}_{N,3},\ (\mathbb{Z}/N)^2 \xrightarrow{\sim} (E^{univ} \times_{\mathcal{M}_{N,3}, g} \mathcal{M}_{N,3})[N]\right)}} \xrightarrow{\sim} (E^{univ}, \alpha^{univ}).$$

$\rightsquigarrow$
$$\begin{tikzcd} E^{univ} \arrow[r, "I_g"] \arrow[d] & E^{univ} \arrow[d] \\ \mathcal{M}_{N,3} \arrow[r, "g", "\sim"'] & E^{univ} \end{tikzcd}$$
cartesian,

Claim We obtain a strictly free group action
$G \circlearrowright E^{univ}$.

Proof of claim. Key pt: compatibility with products gh, $g, h \in G$.

(NB: this is not just a formality and fails for $N = 1, 2$!)

The automorphisms $I_g I_h$ and I_{hg} differ by an element of $\mathrm{Aut}_{\mathcal{M}_{N,3}}(E^{univ}, \alpha^{univ}) = \{id\}$.
$\uparrow N \geq 3$, cf Problem 49.

$\rightsquigarrow$ $-/G$ functorial
$E^{univ}/G \to \mathcal{M}_{N,3}/G$ rel. elliptic ⊛ curve,

α^{univ} induces $(\mathbb{Z}/N)^2 \cong (E^{univ}/G)[N]$

and that pulled back under $\mathcal{M}_{N,3} \to \mathcal{M}_{N,3}/G$ gives back $(E^{univ}, \alpha^{univ})$.

⊛ there remain some things to be checked here...

We obtain a morphism $\mathcal{M}_{N,3}/G \to \mathcal{M}_N$.
Remains to show: isomorphism.

<u>Step 2</u> Take $(E/S, \alpha) \in \mathcal{M}_N(S)$. We show that there exists $f : S \to \mathcal{M}_{N,3}/G$ s.t. $f^*\left(\begin{smallmatrix}\text{universal}\\ \text{object}\end{smallmatrix}\right) \cong (E/S, \alpha)$

(in Step 3 we will show that f unique).

Let $S' \to S$ be the finite étale S-scheme parametrizing level-3 structures on S, a G-torsor,

$$\begin{tikzcd} S' \arrow[r] \arrow[d] \arrow[dr, phantom, "\square"] & \mathcal{M}_3 \arrow[d] \\ S \arrow[r] & \mathcal{M} \end{tikzcd}$$

We obtain $S' \xrightarrow{\tilde{f}} \mathcal{M}_{N,3}$ s.t. the universal $(E^{univ}, \alpha^{univ}, \beta^{univ})$ pulls back to $(E_{S'}/S', \alpha_{S'}$, the universal level-3 str. on $E/S')$.

Then G acts on S', $\mathcal{M}_{N,3}$ and the morphism $S' \to \mathcal{M}_{N,3}$ is G-equivariant. Passing to quotients by G we obtain $S \to \mathcal{M}_{N,3}/G$. By construction of the univ. object on $\mathcal{M}_{N,3}/G$ this has the desired property.

<u>Step 3</u> Show that f in Step 2 is unique:

Consider
$$\begin{tikzcd} S' \arrow[d] & \mathcal{M}_{N,3} \arrow[d] \\ S \arrow[r, "g"] & \mathcal{M}_{N,3}/G \end{tikzcd},$$
S' as in Step 2. Get
$$\begin{tikzcd} S' \arrow[rr] \arrow[dr] & & S \times_{\mathcal{M}_{N,3}/G} \mathcal{M}_{N,3} \arrow[dl] \\ & S & \end{tikzcd}$$

G-equiv. morph of G-torsors$/S$. Every such morphism is an isomorphism.

$\rightsquigarrow$ cartesian diagram

$$\begin{tikzcd} S' \arrow[r, "\tilde{g}"] \arrow[d, "h"'] & \mathcal{M}_{N,3} \arrow[d] \\ S \arrow[r, "g"'] & \mathcal{M}_{N,3}/G. \end{tikzcd}$$

s.t. $\tilde{g}^*(E^{\mathrm{univ}}, \alpha^{\mathrm{univ}}, \beta^{\mathrm{univ}}) \cong (E_{S'}, \alpha_{S'}, \text{univ. level-3 str.})$

$\cong \tilde{f}^*(\ldots)$

with $\tilde{f}$ as in step 2

$\Rightarrow \quad \tilde{g} = \tilde{f}$ by functorial descr. of $\mathcal{M}_{N,3}$

$\Rightarrow \quad gh = fh \quad \underset{\substack{h \text{ étale + surjective} \\ \text{so epimorphism}}}{\Longrightarrow} \quad g = f.$

Finally note that $\mathcal{M}_{N,3}/G$ affine (since $\mathcal{M}_{N,3}$ $\downarrow$ finite étale $\mathcal{M}_3$ $\rightsquigarrow$ $\mathcal{M}_{N,3}$ affine $\rightsquigarrow$ quotient is affine)

and smooth of rel dim 1

$$\left(\begin{tikzcd} \mathcal{M}_{N,3} \arrow[r, "\text{étale}"] \arrow[dr, "\substack{\text{smooth} \\ \text{of rel dim } 1}"'] & \mathcal{M}_{N,3}/G \arrow[d] \\ & \operatorname{Spec} \mathbb{Z}[\frac{1}{3N}] \end{tikzcd} \quad \underset{\substack{[\text{GW2}] \\ \text{Prop } 18.60(2)}}{\longrightarrow} \text{ ok} \right)$$

Remark Similarly one proves the representability of

$$\mathcal{M}_{\Gamma_1(N)} : (\mathrm{Sch}/\mathbb{Z}[\tfrac{1}{N}])^{op} \longrightarrow (\mathrm{Sets})$$

$$S \longmapsto \{(E,P);\ E/S \text{ ell. curve}, \ P \in E[N] \text{ of order } N\}/\cong$$

for $N \geq 4$.

(See [Katz-Mazur] Cor 2.7.4 for the required 'rigidity' result, i.e., $\mathrm{Aut}(E,P) = \{id\}$.)

For an axiomatic description of this result, see [Katz-Mazur] Section 4.7.

Remark The Weil pairing and geometric connected components of $\mathcal{M}_N$.

Recall situation $/\mathbb{C}$: $E/_\mathbb{C} \rightsquigarrow$ Weil pairing $E[N]\times E[N] \xrightarrow{e_N} \mu_N$,

$$\Gamma(N)\backslash \mathbb{H} \overset{1:1}{\hookrightarrow} \left\{ (E, \alpha: (\mathbb{Z}/N)^2 \xrightarrow{\sim} E[N](\mathbb{C})) ;\ e_N\left(\alpha\binom{1}{0}, \alpha\binom{0}{1}\right) = e^{2\pi i/N} \right\} /\cong$$

__Weil pairing__: S scheme, $\mu_{N,S}$ the gp scheme $/S$ of N-th roots of unity $\left(:= \mathbb{Z}[X]/(X^N-1) \underset{\mathbb{Z}}{\times} S\right)$.

E/S elliptic curve

$\rightsquigarrow \quad E[N]\times E[N] \xrightarrow{e_N} \mu_N$ "Weil pairing", alternating non-degenerate pairing.

see [Katz-Mazur] Section 2.8

Different pt of view:

$E \cong E^\vee$

$\rightsquigarrow E[N] \cong \underbrace{E^\vee[N]}$
$\qquad\qquad\quad \| $
$\qquad\qquad E[N]^*$

[Mumford, A.V.], [GW2] Prop. 27.213

$-^* = \mathrm{Hom}(-, \mathbb{G}_m)$ Cartier dual of finite locally free gp scheme

$\rightsquigarrow E[N]\times E[N] \to \mathbb{G}_m$, factors through μ_N

$\rightsquigarrow$ Given $(E/S, \alpha: (\mathbb{Z}/N)^2 \to E[N])$, have well-def'd N-th root of unity $e_N\left(\alpha\binom{1}{0}, \alpha\binom{0}{1}\right) \in \mu_N(S) \subset \Gamma(S, \mathcal{O}_S)^\times$

$\rightsquigarrow \mathcal{M}_N \to \operatorname{Spec} \mathbb{Z}[\tfrac{1}{N}]$ factors through $\operatorname{Spec} \underbrace{\mathbb{Z}[\tfrac{1}{N}, \zeta_N]}$
$$\mathbb{Z}[\tfrac{1}{N}, \zeta_N] = \mathbb{Z}[\tfrac{1}{N}][X]/\Phi_N$$

Thus $\mathcal{M}_N \otimes_{\mathbb{Z}} \mathbb{C}$ decomposes as disjoint union with $\varphi(N)$ connected components.

$e_N\left(\alpha\binom{1}{0}, \alpha\binom{0}{1}\right)$ necessarily primitive N-th root of unity

Can obtain a geometrically connected modular curve $/\mathbb{Z}[\frac{1}{N}, \zeta]$ by setting

$$\mathcal{M}_{N,\zeta} : S \longmapsto \left\{ (E/S, \alpha) \,;\, e_N\left(\alpha\begin{pmatrix}1\\0\end{pmatrix}, \alpha\begin{pmatrix}0\\1\end{pmatrix}\right) = \zeta \right\}.$$

Other interesting questions / topics at this point:

(1) Compactification: Define

$$\begin{array}{ccc} \overline{\mathcal{M}}_N & \xrightarrow{\text{proper}} & \operatorname{Spec} \mathbb{Z}[\tfrac{1}{N}] \\ \text{open dense} \ \cup & \nearrow & \\ \mathcal{M}_N & & \end{array}$$

together with description of $\overline{\mathcal{M}}_N(S)$ in terms of "generalized elliptic curves" (allow singular fibers ...), see [Deligne-Rapoport]

(2) Extend $\mathcal{M}_N$ (and $\overline{\mathcal{M}}_N$) to $\operatorname{Spec} \mathbb{Z}$.

Requires modification of the notion of level-N structure $\rightsquigarrow$ "Drinfeld level structure", see [Katz-Mazur].