Preamble

In July 2019, I attended a retreat of Herwig Hauser's research group in Lüsens (Tyrol) on the topic of *"Moduli"*. In my talk, which in a certain sense served to introduce and motivate the topic of moduli (spaces), I aimed to show how modular curves arising in the classical theory of modular forms can be interpreted as moduli spaces for elliptic curves over the complex numbers. This is essentially the content of the first section below. This "classical" result can also be used as a stepping stone to consider similar moduli problems and to even give a precise definition of what we mean by a "moduli problem" in the first place; this is touched upon in the second section.

1. Contents of the talk in Lüsens

Roughly, a moduli space is a geometric object whose points parametrize a family of objects (up to isomorphism).

A bad example: we could say that $\mathbb{R}^2 \times \mathbb{R}_{>0}$ is a moduli space for circles in the Euclidean plane.

A better example: let $n \geq 0$. Then $\mathbb{P}^{n-1}(\mathbb{C})$ is a moduli space for one-dimensional linear subspaces of $\mathbb{C}^n$.

Today, we talk about the fact that *modular curves are moduli spaces for elliptic curves (with level structure).*

Two fundamental questions: What are elliptic curves?, and: What are modular curves?

1.1. **Definition.** Let k be a field. An *elliptic curve over k* "is" a smooth projective cubic plane curve E over k, together with a distinguished point $O \in E(k)$. I.e.,

$$\begin{aligned} E &= V(F) \\ &= \{[x:y:z] \in \mathbb{P}^2(k) : F(x,y,z) = 0\} \\ &\subset \mathbb{P}^2(k) \end{aligned}$$

for a homogeneous polynomial F of degree 3 with coefficients in k. "Smooth" means that the only solution of $F = \frac{\partial F}{\partial x} = \frac{\partial F}{\partial y} = \frac{\partial F}{\partial z} = 0$ is the trivial one: $x = y = z = 0$.

1.2. **Example.** Consider $E = V(F) \subset \mathbb{P}^2(k)$ in the following cases:

(1) $F(x,y,z) = x^3 + y^3 - z^3$. Smooth: ✓ (as long as $\mathrm{char}(k) \neq 3$). For the distinguished point take e.g. $O = [1:0:1]$. Then (E, O) is an elliptic curve.

(2) $F(x,y,z) = 3x^3 + 4y^3 + 5z^3$. Smooth: ✓ (if $\mathrm{char}(k) \notin \{2,3,5\}$), but if e.g. $k = \mathbb{Q}$ then it was shown by Selmer that $E(k) = \emptyset$, so *there is no choice for O*. (Things would be different if, say, $k = \mathbb{R}$ or $\mathbb{C}$.)

(3) $F(x,y,z) = y^2z - x^3$. Smooth? **No**, because in $[0:1:0] \in E(k)$ all derivatives vanish.

1.3. **Fact.** There is an invariant for curves called the *genus* (dt. *Geschlecht*). For a smooth plane curve C given by a polynomial of degree d, the genus $g = g(C)$ is equal to $\frac{(d-1)(d-2)}{2}$. (If C is not smooth, one has to subtract something depending on the singularities of C.) Thus, a cubic plane curve has genus ≤ 1, and $= 1$ if and only if it is smooth.

On the other hand, it follows from the Riemann-Roch theorem that a smooth curve of genus 1 can be realized as a cubic plane curve (keyword: *Weierstraß normal form*). As a matter of fact, the "proper" definition of elliptic curves over a field k is that they are *smooth projective curves of genus 1 with a distinguished k-rational point O.*

1.4. **Fact.** We just said that for any elliptic curve, the defining equation can be put in Weierstraß form. We are not going to need this form in full generality; it suffices to know that, if $\mathrm{char}(k) \neq 2, 3$, then by a linear change of coordinates the equation can be (further) simplified to

$$y^2 = 4x^3 + Ax + B$$

(or more precisely its homogenization) with distinguished point the "point at infinity" $O = [0:1:0]$. Smoothness of E implies that the *discriminant* $\Delta = -16(4A^3 + 27B^2)$ is nonzero (and viceversa, every equation of this form with this condition on the coefficients yields a smooth cubic). The quantity $j(E) = -12^3 \cdot \frac{64A^3}{\Delta}$ can be shown to be invariant under isomorphism (which is why it's called the *j-invariant*). Conversely, it turns out that if two elliptic curves over an algebraically closed field have the same j-invariant, then they are already isomorphic.

1.5. Now we should define modular curves. This is done as follows: first, consider the action of $\mathrm{GL}_2(\mathbb{R})$ on $\mathbb{P}^1(\mathbb{C})$ " $= \mathbb{C} \cup \{\infty\}$ " given by fractional linear transformations,

$$\gamma \cdot z := \frac{az+b}{cz+d}, \qquad \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{R}).$$

(Special cases: let $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ be given. If $c \neq 0$, then $\gamma \cdot \left(-\frac{d}{c}\right) = \infty$ and $\gamma \cdot \infty = \frac{a}{c}$. If $c = 0$, then $\gamma \cdot \infty = \infty$.)

If $\det \gamma > 0$ and $\mathrm{Im}(z) > 0$ (in particular, $\gamma \cdot z \neq \infty$), then a simple computation shows that $\mathrm{Im}(\gamma \cdot z) > 0$. In other words, $\mathrm{GL}_2(\mathbb{R})^+$, or any subgroup thereof, acts on the upper half-plane $\mathfrak{H} := \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\} \subset \mathbb{C}$.

1.6. **Definition.** (1) $\mathrm{SL}_2(\mathbb{Z})$ and its subgroups of finite index are called *modular groups*. The *full modular group* is $\mathrm{SL}_2(\mathbb{Z})$.

(2) For a non-negative integer N, the subgroup

$$\begin{aligned}\Gamma(N) &= \ker(\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}))\\ &= \left\{\gamma \in \mathrm{SL}_2(\mathbb{Z}) : \gamma \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{N}\right\}\end{aligned}$$

is of finite index in $\mathrm{SL}_2(\mathbb{Z})$; it is called the *principal congruence subgroup of level N* (dt. *Hauptkongruenzuntergruppe der Stufe N*). Observe that $\Gamma(1) = \mathrm{SL}_2(\mathbb{Z})$.

(3) Let $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$, $\Gamma \supseteq \Gamma(N)$ for some N. The quotient of $\mathfrak{H}$ by the action of Γ, denoted $Y(\Gamma)$, is the *modular curve* (dt. *Modulkurve*) corresponding to Γ. In the special case $\Gamma = \Gamma(N)$ the corresponding modular curve is denoted simply $Y(N)$.

(4) For a non-negative integer N, consider the *Hecke modular groups*

$$\Gamma_0(N) = \left\{\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : c \equiv 0 \pmod{N}\right\}$$

and

$$\Gamma_1(N) = \left\{\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : c \equiv 0 \pmod{N},\ a \equiv d \equiv 1 \pmod{N}\right\}.$$

Observe that $\Gamma(N) \subseteq \Gamma_1(N) \subseteq \Gamma_0(N)$ for all N. The corresponding modular curves are denoted $Y_0(N)$ and $Y_1(N)$, respectively.

1.7. Why are the modular curves *curves*?, one may ask. Because, since $\mathfrak{H}$ is an open subset of $\mathbb{C}$, and Γ acts *properly discontinuously* (dt. *eigentlich diskontinuierlich*), the quotient inherits a differentiable structure, i.e., it is a (one-dimensional) *complex manifold* in a natural way. (In other words, it is a topological space that is locally homoeomorphic to the open unit disk in $\mathbb{C}$ and such that transition maps between charts are holomorphic.) As a one-dimensional manifold, it is a "curve".

1.8. We shall now show that the points of the modular curve $Y_0(1) = \mathrm{SL}_2(\mathbb{Z})\backslash\mathfrak{H}$ (it is customary to write the quotient "on the left") parametrize isomorphism classes of elliptic curves over $\mathbb{C}$. The claim follows by combining the facts below:

1.9. **Fact.** (1) Let $\Lambda \subset \mathbb{C}$ be a *lattice* (dt. *Gitter*) in $\mathbb{C}$, i.e. a discrete subgroup of rank 2 (i.e., $\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$ for complex numbers ω_1, ω_2 which are $\mathbb{R}$-linearly independent). Then the quotient $\mathbb{C}/\Lambda$, with $0 \in \mathbb{C}/\Lambda$ as its distinguished point, is an elliptic curve over $\mathbb{C}$ given by (the homogenization of) the equation

$$y^2 = 4x^3 - g_2x - g_3,$$

where $g_2 = g_2(\Lambda) = 60\sum_{0\neq l\in\Lambda}\frac{1}{l^4}$ and $g_3 = g_3(\Lambda) = 140\sum_{0\neq l\in\Lambda}\frac{1}{l^6}$, and conversely every elliptic curve over $\mathbb{C}$ is of this form.

(2) Two elliptic curves E, E' over $\mathbb{C}$ are isomorphic if and only if the corresponding lattices Λ, Λ' are *homothetic*, i.e., there exists a complex number λ with $\Lambda' = \lambda\Lambda$.

(3) Every lattice is homothetic to a lattice $\Lambda_\tau = \mathbb{Z} \oplus \tau\mathbb{Z}$ for some $\tau \in \mathfrak{H}$. (*Caveat*: there is more than one τ for which this holds! For instance, it is easy to see that $\Lambda_\tau = \Lambda_{1+\tau}$ for any $\tau \in \mathfrak{H}$.)

(4) Two lattices Λ_τ and $\Lambda_{\tau'}$ are the same (up to homothety) if and only if $\tau' = \frac{a\tau+b}{c\tau+d}$ for some $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$.

1.10**.** About the proofs:

(1) By general theory, there is a one-to-one correspondence between smooth projective algebraic curves over $\mathbb{C}$ and compact (connected) one-dimensional complex manifolds. When the complex manifold is viewed as a real surface, it is a *closed surface* (dt. *geschlossene Fläche*) and it is orientable, and so by a well-known classification it is homoeomorphic to a sphere with a finite number of "handles". This number is called the *genus* of the surface and turns out to be precisely equal to the (algebraic) genus mentioned above. Thus, elliptic curves over $\mathbb{C}$ "are" complex tori. And a torus is a parallelogramme with opposite sides identified, i.e. a quotient $\mathbb{C}/\Lambda$ for a lattice Λ. The exact equation is obtained by the theory of elliptic functions and involves the *Weierstraß* $\wp$ *function.* To go back, one uses the fact that the j-invariant is surjective (i.e., each complex number appears as the j-invariant of some elliptic curve over $\mathbb{C}$).

(2) It turns out that two lattices are homothetic if and only if the corresponding j-invariants are equal.

(3) This is easy: if $\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$, then choose $\tau \in \{\frac{\omega_1}{\omega_2}, \frac{\omega_2}{\omega_1}\}$ so that $\mathrm{Im}(\tau) > 0$ and accordingly $\lambda = \omega_2$ or $\lambda = \omega_1$.

(4) In general, two bases $\{\omega_1, \omega_2\}$ and $\{\omega_1', \omega_2'\}$ define the same lattice if and only if there is an invertible matrix with coefficients in $\mathbb{Z}$ converting one basis representation into the other. If furthermore the bases are ordered so that $\omega_1/\omega_2 = \tau \in \mathfrak{H}$ and similarly for the other one, then the determinant of the base change matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ must be positive (hence $+1$) and $\tau' = \frac{\omega_1'}{\omega_2'} = \frac{a\omega_1+b\omega_2}{c\omega_1+d\omega_2} = \frac{a\tau+b}{c\tau+d}$ as claimed.

2. Formalization of moduli problems

We have seen in the previous section that points of $Y_0(1) = \mathrm{SL}_2(\mathbb{Z})\backslash\mathfrak{H}$ parametrize isomorphism classes of elliptic curves over $\mathbb{C}$. Thus, according to our initial "definition", $Y_0(1)$ is "a moduli space" for elliptic curves over $\mathbb{C}$. But we have also seen that isomorphism classes of elliptic curves over $\mathbb{C}$ are parametrized by the set of values attained by the j-invariant, which is a subset of the complex numbers. In fact, it turns out that the map $j : \mathfrak{H} \to \mathbb{C}$ sending $\tau \in \mathfrak{H}$ to the j-invariant of the elliptic curve $\mathbb{C}/(\mathbb{Z} \oplus \tau\mathbb{Z})$ is surjective, and so we could've taken $\mathbb{C}$ itself to be a moduli space for elliptic curves over $\mathbb{C}$. But then *why would we bother with modular curves*, when $\mathbb{C}$ is obviously an "easier" moduli space? What is the advantage in using one space rather than the other?

2.1. One advantage of the description by modular curves is that it generalizes, in the sense that *every modular curve of the form* $Y_0(N)$*,* $Y_1(N)$ *or* $Y(N)$ as introduced in 1.6 *can be interpreted as a moduli space for elliptic curves over* $\mathbb{C}$ *with additional structure.* In order to thoroughly explain this, we have to look more closely at the group law on elliptic curves.

Let (E, O) be an elliptic curve over k. Then the set $E(k)$ of k-rational points of E can be made into an abelian group with zero element given by the distinguished point $O \in E(k)$. The deeper reason for this stems from E having genus one: in fact, by the Riemann-Roch theorem, the choice of O yields a bijection between the points of E and the abelian group of degree-zero divisors on E, so we can "pull back" the group structure onto (the underlying set of) E. (Although we won't need this, the maps describing multiplication and inversion are even morphisms of varieties, so an elliptic curve is actually an *algebraic group.*) However, the group law also has a very concrete description: once we bring the describing equation for E in Weierstraß form (hereby sending O to the point $[0 : 1 : 0]$), the point O acts as the neutral element and any three points $P, Q, R \in E(k)$ sum up to O if and only if they are collinear in $\mathbb{P}^2(k)$. Finally, over $k = \mathbb{C}$ there is an even simpler description available: if $E \cong \mathbb{C}/\Lambda$, then the group law on E is obtained by pulling back the group law on the quotient group $\mathbb{C}/\Lambda$.

The last description allows us to analyze the N-torsion on E, denoted $E[N]$, for any positive integer $N \geq 1$, at least over the ground field $k = \mathbb{C}$. If we let $\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$ be a lattice such that $E \cong \mathbb{C}/\Lambda$, then obviously any complex number which is a $\mathbb{Z}$-linear combination of $\frac{\omega_1}{N}$ and $\frac{\omega_2}{N}$ gives rise to an element in the torsion $E[N] \subset E$. In more succinct terms,

$$E[N] = \frac{1}{N}\Lambda/\Lambda$$

and in particular $E[N]$ is a free $\mathbb{Z}/N\mathbb{Z}$-module of rank 2. For a lattice of the form $\Lambda = \Lambda_\tau = \mathbb{Z} \oplus \tau\mathbb{Z}$, we see immediately that $1/N$ and τ/N form a basis for $E[N]$. We finally introduce the *Weil pairing*

$$e : E[N] \times E[N] \to \mathbb{Z}/N\mathbb{Z}$$

sending a pair (P, Q) with $P = a\frac{\omega_1}{N} + b\frac{\omega_2}{N}$ and $Q = c\frac{\omega_1}{N} + d\frac{\omega_2}{N}$ to the element

$$e(P, Q) := ad - bc \in \mathbb{Z}/N\mathbb{Z}.$$

Note that, for the special choice $\Lambda = \Lambda_\tau$, one has $e(1/N, \tau/N) = -1$.

2.2. At this point, for any integer $N \geq 1$ (the "level") we can define *level-N structures* on E in the following ways:

(1) We can take a level-N structure to be a pair (E, P) where P is a point of $E(k)$ of exact order N. Two such pairs are isomorphic if there is an isomorphism $\phi : E \to E'$ sending P to P'.

(2) We can take a level-N structure to be a pair (E, C) where C is a cyclic subgroup of E of order N. Two such pairs are isomorphic if there is an isomorphism $\phi : E \to E'$ such that $\phi(C) = C'$.

(3) We can take a level-N structure to be a triple (E, P, Q) where P and Q are a basis for $E[N]$ with $e(P, Q) = -1$. Two such triples are isomorphic if there is an isomorphism $\phi : E \to E'$ sending P to P' and Q to Q'.

(Observe that the first two notions make sense for elliptic curves over any field, and that, for $N = 1$, any of the three notions collapses to the definition of an elliptic curve.)

Using the above result – i.e., the bijection by which the orbit of $\tau \in \mathfrak{H}$ in $\mathrm{SL}_2(\mathbb{Z})\backslash\mathfrak{H}$ corresponds to the isomorphism class of the elliptic curve $\mathbb{C}/\Lambda_\tau$ – and keeping track of what happens to the special point(s) P (and Q), resp. the subgroup C, it is not especially hard to prove the following statements, see e.g. the first two and a half pages of [3] or alternatively [1, §7.2].

2.3. **Fact.** Let $N \geq 1$ be an integer.

(1) The points of the modular curve $Y_1(N)$ parametrize isomorphism classes of pairs (E, P) as above.

(2) The points of the modular curve $Y_0(N)$ parametrize isomorphism classes of pairs (E, C) as above.

(3) The points of the modular curve $Y(N)$ parametrize isomorphism classes of triples (E, P, Q) as above.

2.4. We have now essentially proved the claim that we started out with: modular curves are moduli spaces for elliptic curves with level structure. The word "essentially" is crucial because *we still have not defined what we mean by a moduli space* or rather *what properties we expect (read: demand) that a moduli space should have.* Nonetheless, the correspondences we have observed so far will be enough to attain a formal definition.

To proceed towards formalization, recall that a moduli space should be a space of some kind (!) whose points parametrize isomorphism classes of a certain type of object. It is only natural to require that, if the objects we wish to classify (e.g., in our case, elliptic curves over $\mathbb{C}$) belong to some category (that of algebraic varieties over $\mathbb{C}$), then so should the moduli space $\mathcal{M}$. But then, if $\mathcal{M}$ is an algebraic variety over the algebraically closed field $\mathbb{C}$, its (closed) points have a more conceptual interpretation as morphisms (of schemes!) $\operatorname{Spec}\mathbb{C} \to \mathcal{M}$. We thus have the following situation: starting e.g. from the base field $\mathbb{C}$, we have on the one hand a family $\mathcal{F}(\mathbb{C})$ of objects to be classified (considered as a set) and on the other hand we seek an algebraic variety $\mathcal{M}$ such that

$$\operatorname{Hom}(\operatorname{Spec}\mathbb{C}, \mathcal{M})$$

(again considered as a set) is isomorphic (as a set!) to $\mathcal{F}(\mathbb{C})$. This suggests a "categorification", as we shall see presently.

2.5. Recall the following basic notions. Let $\mathcal{C}$ be a category and A be an object of $\mathcal{C}$. If $\mathcal{C}$ is *locally small*, then this means (almost by definition) that for any object B of $\mathcal{C}$ we have a corresponding set (i.e., object in the category **Set**) $\operatorname{Hom}_{\mathcal{C}}(A, B)$. Moreover, for a morphism $\phi : B \to B'$ in $\mathcal{C}$, we have a corresponding morphism $\operatorname{Hom}_{\mathcal{C}}(A, B) \to \operatorname{Hom}_{\mathcal{C}}(A, B')$ which sends $\psi \in \operatorname{Hom}_{\mathcal{C}}(A, B)$ to the composition $\phi \circ \psi \in \operatorname{Hom}_{\mathcal{C}}(A, B')$. These assignments determine a *covariant functor* $\mathcal{C} \to$ **Set**, which we denote by $\operatorname{Hom}_{\mathcal{C}}(A, -)$. Similarly, any object B of $\mathcal{C}$ determines a *contravariant functor* $\operatorname{Hom}_{\mathcal{C}}(-, B)$ from $\mathcal{C}$ to **Set**. We say that the former (resp., latter) functor is *represented* by A (resp., B), and functors of this form[1] are said to be *representable.*

Let us again look at the situation of 2.4. The step where we have put the points of $\mathcal{M}$ in bijection with the elements of $\operatorname{Hom}(\operatorname{Spec}\mathbb{C}, \mathcal{M})$ suggests that the right category in which to work is that of *schemes* (or some full subcategory, for instance the one of *Noetherian schemes*). If we manage to extend the above assignment $\mathbb{C} \mapsto \mathcal{F}(\mathbb{C})$ – or rather, after an obvious shift in perspective, $\operatorname{Spec}\mathbb{C} \mapsto \mathcal{F}(\operatorname{Spec}\mathbb{C})$ – to a contravariant functor $\mathcal{F}$ from the category of Noetherian schemes to **Set**, then we will (finally) be able to give a proper definition of a moduli space, namely as a scheme representing $\mathcal{F}$ (if it exists). This is now *precisely* the line of reasoning that leads to the formalization

[1] up to a *natural isomorphism*

of moduli problems: compare the two definitions below, taken from [4, Chapter 5, §2] and from [2, Chapter 4], respectively.

2.6. **Definition** (after Mumford). Let $g \geq 0$ be an integer.

(1) Let S be a Noetherian schemes. A smooth, proper morphism of schemes $C \to S$ is called a *curve of genus g over S* if all its geometric fibers are irreducible curves of genus g. Let $\mathscr{M}_g(S)$ denote the set of curves of genus g over S.

(2) Given a morphism $f : T \to S$ of Noetherian schemes and a curve $C \to S$ of genus g over S, one checks that the projection from the fibre product $C \times_S T$ to its second factor T defines a curve of genus g over T. Thus, f induces a map from $\mathscr{M}_g(S)$ to $\mathscr{M}_g(T)$, which we denote by $\mathscr{M}_g(f)$.

(3) The previous observations combined yield a contravariant functor $\mathscr{M}_g$ from the category of Noetherian schemes to **Set**. If this functor is representable by a scheme $\mathcal{M}$, we call $\mathcal{M}$ a *fine moduli scheme.*

(4) Mumford also defines what it means for a scheme to be a *coarse moduli scheme* (for a particular moduli problem); the gist of this latter definition is that, when specializing to (spectra of) algebraically closed fields, we still obtain a bijection as wished, and the "universality" of the moduli scheme is made (more) explicit, but the resulting notion is weaker than its "fine" counterpart from (3).[2]

2.7. **Definition** (after Katz-Mazur). Recall that an elliptic curve over a field k is a smooth projective curve E of genus 1 over k together with a k-rational point. In the language of schemes, this means a (smooth etc.) morphism of schemes $E \to \operatorname{Spec} k$ together with a section $O : \operatorname{Spec} k \to S$.

(1) Let S be an arbitrary scheme. An *elliptic curve over S* is a smooth, proper morphism of schemes $E \to S$ all of whose geometric fibers are irreducible curves of genus 1, together with a section O.

(2) A morphism of elliptic curves $E \to S$ and $E' \to S'$ is a cartesian (!) square

$$\begin{tikzcd}
E' \arrow[r] \arrow[d] & E \arrow[d] \\
S' \arrow[r] & S.
\end{tikzcd}$$

Recall that "cartesian" means that E' is isomorphic to the fibre product $E \times_S S'$.

(3) Elliptic curves over variable base schemes, together with their morphisms, form a category **Ell**. A *moduli problem for elliptic curves* is a contravariant functor $\mathcal{P}$:

[2] On the other hand, Mumford calls the definition of a fine moduli scheme "vacuous", and that of a coarse moduli scheme the "useful" one.

Ell → **Set**. We call a moduli problem $\mathcal{P}$ *representable* if it is so as a contravariant functor.

2.8. **Caveat.** The two definitions above involve representability of *different functors* (between *different categories*!) and so cannot quite be compared directly. See [2, (4.3)–(4.4)] for an explanation of how a representable moduli problem in the sense of Def. 2.7 yields a scheme representing a functor as in Def. 2.6 (i.e., a fine moduli scheme). One obtains a converse if $\mathcal{P}$ is *rigid*, see *ibid.*

2.9. **Remark.** The category **Ell** from 2.7 is called the *moduli stack of elliptic curves.* It is a special case of an *algebraic stack* and can be seen as one of the main motivations for introducing such objects. This links nicely to the article [6] Christopher suggested to me prior to the workshop.

2.10**.** "Categorifying" the problem has several desirable consequences beside offering an elegant reformulation:

(1) It allows us to talk about families of elliptic curves, as shown by the following example (taken from [1, Example 8.1.1]). If e.g. we put

$$S = \operatorname{Spec}(\mathbb{Z}[j, j^{-1}(j-1728)^{-1}])$$

and let E be the closed subscheme of $\mathbb{P}^2_S$ defined by (the homogenization of)

$$y^2 + xy = x^3 - \frac{36}{j-1728}x - \frac{1}{j-1728},$$

then E is an elliptic curve over S: for each geometric point $\operatorname{Spec}\Omega \to S$, defined by a ring morphism $j \mapsto j_0 \in \Omega$, $j_0 \neq 0, 1728$, the fibre is an elliptic curve with j-invariant j_0, obtained by replacing j with j_0 in the Weierstraß equation.

(2) It allows us to talk about level structures (!).

In the picture of Def. 2.6, this is achieved by specializing to the subcategory of $\mathbb{Z}[1/N]$-schemes and then finding appropriate "replacements" for pairs (E, P) resp. (E, C) (cf. 2.2); see [1, 8.2] for more details. We borrow their notation $(\mathcal{E}, \mathcal{P})$, resp. $(\mathcal{E}, \mathcal{C})$, for these newly-defined pairs.

In the picture of Def. 2.7, given a moduli problem $\mathcal{P}$, a *"level $\mathcal{P}$ structure"* on an object $E \to S$ of **Ell** is an element of the set $\mathcal{P}(E \to S)$.

2.11**.** Let us finally talk (more) rigorously about moduli spaces. We refer to [1, 8.2] and [2, Chapter 4] for more details.

2.12. **Fact.** (1) Let $\mathscr{F}_1(N)$ be the contravariant functor from the category of $\mathbb{Z}[1/N]$-schemes to **Set** which assigns to S the set of isomorphism classes of pairs $(\mathcal{E}, \mathcal{P})$, cf.

2.10.(2). Then for $N > 3$ the functor $\mathscr{F}_1(N)$ is representable (i.e., we have a fine moduli scheme). Moreover, the $\mathbb{C}$-points of this moduli scheme form a space analytically isomorphic to $Y_1(N)$.

(2) Let $\mathscr{F}_0(N)$ be the contravariant functor from the category of $\mathbb{Z}[1/N]$-schemes to **Set** which assigns to S the set of isomorphism classes of pairs $(\mathcal{E}, \mathcal{C})$, cf. again 2.10.(2). Then one can construct a scheme which is a coarse moduli scheme, and whose space of $\mathbb{C}$-points is analytically isomorphic to $Y_0(N)$; however, it need not represent $\mathscr{F}_0(N)$ in general.

(3) In the case $N = 1$ it even turns out that *there cannot be a fine moduli scheme* because elliptic curves have nontrivial automorphisms, as explained in [5], [6].[3] The problem however becomes solvable when passing to the level of stacks, as explained in [6].

2.13. **Remark.** Let us conclude with a remark that is most interesting if one is already familiar with the theory of modular curves.

Let $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ be a congruence subgroup, meaning that $\Gamma \supseteq \Gamma(N)$ for some $N \geq 1$. Recall that the modular curve $Y(\Gamma) = \Gamma \backslash \mathfrak{H}$ has the structure of a one-dimensional complex manifold.

In the classical theory of modular curves, one learns that $Y(\Gamma)$ has a *compactification* $X(\Gamma)$ that is obtained by adding finitely many points, called the *cusps* of $\Gamma \backslash \mathfrak{H}$, just like $\mathbb{C}$ is compactified by adding the single point ∞ to obtain the *Riemannsche Zahlenkugel.*

One can construct $X(\Gamma)$ directly, namely as the quotient $\Gamma \backslash \mathfrak{H}^*$, where

$$\mathfrak{H}^* := \mathfrak{H} \cup \mathbb{Q} \cup \{\infty\} \subset \mathbb{P}^1(\mathbb{C}).$$

This space is indeed the disjoint union of $\Gamma \backslash \mathfrak{H}$ and a finite set of points. By defining suitable open charts at each point, $\Gamma \backslash \mathfrak{H}^*$ is given the desired structure of a one-dimensional complex manifold, which turns out to be compact.

Since we have a (loose) moduli interpretation for modular curves of the form $Y(N)$, $Y_0(N)$ and $Y_1(N)$ for any $N \geq 1$, it is natural to wonder if there is an analogous, "compatible" interpretation of their respective compactifications $X(N)$, $X_0(N)$, $X_1(N)$, and if so, what the cusps correspond to. This is answered in [1, 9.2 and 9.3]: briefly, we can say that, when a point of $Y_0(1) = \mathrm{SL}_2(\mathbb{Z}) \backslash \mathfrak{H}$ gets closer to a cusp, the corresponding elliptic curve gets closer to being "degenerate", and so we can weaken our definition

[3] In fact, the notion of *rigidity* of a moduli problem $\mathcal{P}$ as in Def. 2.7 – which, as we mentioned in 2.8, guarantees that a representable moduli problem admits a fine moduli scheme – boils down precisely to the absence of nontrivial automorphisms.

of elliptic curves to include the degenerate cases (this is then called a *generalized elliptic curve*, again over a base scheme S) and consider, similarly to what we did above, the moduli problem for isomorphism classes of *generalized* elliptic curves with level structure. It turns out that coarse moduli schemes always exist both for pairs $(\mathcal{E}, \mathcal{P})$ and for pairs $(\mathcal{E}, \mathcal{C})$ and that their spaces of $\mathbb{C}$-points are analytically isomorphic to the compactified modular curves $X_1(N)$ and $X_0(N)$, respectively. In the case of pairs $(\mathcal{E}, \mathcal{P})$ and for $N > 4$ the moduli scheme is even a fine one.

References

[1] Fred Diamond and John Im, *Modular forms and modular curves*, Seminar on Fermat's Last Theorem, Providence, RI, 1995, pp. 39–133. Available online at https://www.math.wisc.edu/~boston/Diamond-Im-Modular_forms_and_modular_curves.pdf.

[2] Nicholas M. Katz, Barry Mazur, *Arithmetic Moduli of Elliptic Curves*, Ann. Math Studies **108**, Princeton Univ. Press, Princeton, 1985.

[3] Kenneth A. Ribet, William A. Stein, *Points on modular curves parameterize elliptic curves with extra structure*, lecture notes. Available online at https://wstein.org/edu/Fall2003/252/lectures/09-24-03/moduli_and_ramification.pdf.

[4] John Fogarty, Frances Kirwan, David Mumford, *Geometric Invariant Theory*, Third Enlarged Edition, Ergebnisse der Mathematik und Ihrer Grenzgebiete **34**, Springer Berlin Heidelberg, 1994.

[5] nLab, *Moduli space*, https://ncatlab.org/nlab/show/moduli+space.

[6] Dan Edidin, *What Is. . . A Stack?*, Notices of the AMS, Vol. 50, No. 4. Available online at https://www.ams.org/notices/200304/what-is.pdf.