Moduli of elliptic curves

Peter Bruin
12 September 2007

1. Elliptic curves over schemes

The notion of elliptic curves over arbitrary schemes is indispensable for the topic of moduli spaces. Intuitively speaking, we can describe an elliptic curve over a scheme S as an "algebraic family" of elliptic curves, one for each point of S.

Definition. Let k be an algebraically closed field. An *elliptic curve* over k is a pair (E, O) with E a proper smooth curve over k which is connected and of genus 1, i.e. $\dim_k \mathrm{H}^1(E, \mathcal{O}_E) = 1$ (or equivalently, by smoothness and Serre duality, $\dim_k \Omega^1_{E/k}(E) = 1$), and with $O \in E(k)$ a rational point.

Every elliptic curve (E, O) has in a natural the structure of a commutative group scheme over k with unit O. Furthermore, it is known that E can be embedded in the projective plane over k as the curve defined by a *generalised Weierstrass equation*

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3$$

with O corresponding to the point with projective coordinates $(0 : 1 : 0)$.

Definition. Let S be a scheme. An *elliptic curve* over S is a proper smooth morphism of schemes $p\colon E \to S$ whose fibres are geometrically connected curves of genus 1, together with a section $O \in E(S)$.

In other words, an elliptic curve over S is a morphism $p\colon E \to S$ which is finitely presented, proper and flat, together with a section $O \in E(S)$, such that the geometric fibres (together with the points obtained by specialising O) are elliptic curves in the sense of the first definition. (The finiteness of presentation follows from the conditions of finite type, separatedness and locally finite presentation, which are implicit in the conditions of properness and smoothness.)

Elliptic curves "persist under base change": if $(p\colon E \to S, O)$ is an elliptic curve, and $S' \to S$ is any morphism of schemes, then the scheme $E_{S'} = E \times_S S'$, viewed as an S'-scheme, is (together with the section $O_{S'}\colon S' \to E_{S'}$) an elliptic curve over S'. This follows from the fact that properness, smoothness, and the property of the geometric fibres being connected curves of genus 1 are preserved under base change.

Example. Consider the affine scheme

$$S = \operatorname{Spec} \mathbf{Z}\left[\frac{1}{2}, a, b, \frac{1}{4a^3 + 27b^2}\right],$$

and let $E \subset \mathbf{P}^2_S$ be defined by

$$y^2z = x^3 + axz^2 + bz^3$$

together with the point $O = (0 : 1 : 0)$. The pair (E, O) is an elliptic curve over S.

Like in the case of a field as the base scheme, an elliptic curve over an arbitrary scheme S has a natural structure of commutative group scheme over S; see Deligne and Rapoport [2], II, proposition 2.7, or Katz and Mazur [3], Theorem 2.1.2. It is no longer the case that every elliptic curve E/S can be embedded in $\mathbf{P}^2_S$ via a Weierstrass equation, but such an embedding does exist over sufficiently small open subschemes of S; see [3], § 2.2.

Definition. The *category of elliptic curves*, denoted by **Ell**, is defined as follows. The objects of **Ell** are elliptic curves $(p\colon E \to S, O)$ over variable base schemes S; we will often use the abbreviation E/S. The morphisms from $(p'\colon E' \to S', O')$ to $(p\colon E \to S, O)$ are the pairs $(f\colon S' \to S, g\colon E' \to E)$ such that the diagram

$$\begin{array}{ccc} E' & \xrightarrow{g} & E \\ {\scriptstyle p'}\downarrow & & \downarrow{\scriptstyle p} \\ S' & \xrightarrow{f} & S \end{array}$$

is Cartesian and the section $O_{S'}\colon S' \to E'$ induced by O equals O'. For the sake of brevity, we will leave the requirement on O and O' implicit from now on.

Remark. The category **Ell** is a smooth Deligne–Mumford stack for the *fpqc*-topology on the category of schemes; see Deligne and Rapoport [2], III, théorème 2.5. In these notes we will not use the language of stacks, but rather that of *relatively representable moduli problems* introduced by Katz and Mazur [3].

Fact 1.1. *Products exist in the category* **Ell**, *i.e. given two elliptic curves $E \to S$ and $E' \to S'$, there exists an elliptic curve $E'' \to S''$ with morphisms to E/S and E'/S' such that the natural map of sets*

$$\mathrm{Hom}_{\mathbf{Ell}}(F/T, E''/S'') \to \mathrm{Hom}_{\mathbf{Ell}}(F/T, E/S) \times \mathrm{Hom}_{\mathbf{Ell}}(F/T, E'/S')$$

is an isomorphism for all elliptic curves $F \to T$.

(The proof of this fact comes down to the representability of $\mathbf{Isom}_{S\times S'}(p_1^*E, p_2^*E')$ as a scheme; cf. Deligne and Rapoport [2], III, théorème 2.5. It uses the theory of Hilbert schemes, which I don't know enough about to give the proof.)

2. Representable functors

Let $\mathcal{C}$ be a category, and let $F\colon \mathcal{C} \to \mathbf{Sets}$ be a contravariant functor. We say that F is *representable* if there exists an object X of $\mathcal{C}$ such that F is isomorphic to the (contravariant) functor

$$\begin{aligned} h^X\colon \mathcal{C} &\to \mathbf{Sets} \\ T &\mapsto \mathrm{Hom}_{\mathcal{C}}(T, X). \end{aligned}$$

We also say that F is *represented* by the object X. It follows from Yoneda's lemma that this object is unique up to unique isomorphism.

Example. Let **Sch** be the category of schemes, and consider the functor

$$\begin{aligned} \mathbf{G}_{\mathrm{m}}\colon \mathbf{Sch} &\to \mathbf{Sets} \\ S &\mapsto \mathcal{O}_S(S)^\times. \end{aligned}$$

This functor is representable by the affine scheme $\operatorname{Spec} \mathbf{Z}[x, 1/x]$. (In this example, the functor $\mathbf{G}_{\mathrm{m}}$ factors via the category of Abelian groups; this gives the representing scheme the structure of a commutative group scheme.)

Example. Suppose products exist in the category $\mathcal{C}$. If $F\colon \mathcal{C} \to \mathbf{Sets}$ and $G\colon \mathcal{C} \to \mathit{Sets}$ are represented by objects X and Y, respectively, then the functor

$$\begin{aligned} F \times G\colon \mathcal{C} &\to \mathbf{Sets} \\ T &\mapsto F(T) \times G(T) \end{aligned}$$

is represented by the product of X and Y.

3. Moduli problems

Definition. A *moduli problem* (for elliptic curves) is a contravariant functor

$$\mathcal{P}\colon \mathbf{Ell} \to \mathbf{Sets}.$$

An element of $\mathcal{P}(E/S)$ is called a *$\mathcal{P}$-structure* on the elliptic curve E over S. The category of *elliptic curves with $\mathcal{P}$-structure*, denoted by $\mathbf{Ell}_{\mathcal{P}}$, is defined as follows: the objects are the pairs $(E \to S, \alpha)$ with $E \to S$ an elliptic curve and α an element of $\mathcal{P}(E/S)$, and the morphisms from $(E' \to S', \alpha')$ to $(E \to S, \alpha)$ are the elements $\phi \in \mathrm{Hom}_{\mathbf{Ell}}(E'/S', E/S)$ such that the function of sets $F(\phi)\colon F(E/S) \to F(E'/S')$ maps α to α'. There is a "forgetful functor"

$$F_{\mathcal{P}}\colon \mathbf{Ell}_{\mathcal{P}} \to \mathbf{Ell}$$

sending a pair $(E \to S, \alpha)$ to the elliptic curve $E \to S$.

Since $\mathcal{P}$ is a functor, we can ask the question whether it is representable. This turns out to be a very useful thing to do. First of all, every elliptic curve $E \to S$ over some base scheme S defines a representable moduli problem, namely

$$h^{E/S} = \mathrm{Hom}_{\mathbf{Ell}}(\quad, E/S),$$

given by

$$h^{E/S}(E'/S') = \left\{ \big(f\colon S' \to S, g\colon E' \to E\big) \;\middle|\; \text{the square } \begin{array}{ccc} E' & \xrightarrow{g} & E \\ \downarrow & & \downarrow \\ S' & \xrightarrow{f} & S \end{array} \text{ is Cartesian} \right\}$$

for every elliptic curve $E' \to S'$. Imitating the terminology of $\mathcal{P}$-structures introduced above in the case $\mathcal{P} = h^{E/S}$, we will call an element of $h^{E/S}(E'/S')$ an *E/S-structure* on E'/S'. We define the category of *elliptic curves with E/S-structure*, denoted by $\mathbf{Ell}_{E/S}$, by taking as objects the Cartesian squares

$$\begin{array}{ccc} E' & \xrightarrow{g'} & E \\ \downarrow & \square & \downarrow \\ S' & \xrightarrow{f'} & S \end{array}$$

and by taking as morphisms from $(E'' \to S'', f'', g'')$ to $(E' \to S', f', g')$ the morphisms $(\hat{f}, \hat{g}) \in \mathrm{Hom}_{\mathbf{Ell}}(E''/S'', E'/S')$ such that $f'\hat{f} = f''$ and $g'\hat{g} = g''$ (i.e. giving a "commutative prism with Cartesian squares"). This category is canonically isomorphic to $\mathbf{Ell}_{h^{E/S}}$, and the forgetful functor $F_{h^{E/S}}$ corresponds under this isomorphism to the functor

$$F_{E/S}\colon \mathbf{Ell}_{E/S} \to \mathbf{Ell}$$

sending a Cartesian diagram as above to E'/S'.

We can also talk about moduli problems for elliptic curves over B-schemes, where B is an arbitrary base scheme (instead of $\mathbf{Z}$); this makes no essential difference for the results we will discuss (i.e. they remain valid if 'scheme' is replaced by 'B-scheme' in all relevant places). The cases $B = \mathbf{Z}[1/n]$ and $B = \mathbf{Z}[1/n, \zeta_n]$, with ζ_n a primitive n-th root of unity, and $B = \mathbf{F}_p$, with p a prime number, are often useful.

4. An example of a representable moduli problem

Let $[\Gamma(3)]$ be the moduli problem on $\mathbf{Z}[1/3]$-schemes given by

$$E/S \longmapsto \{\, \text{isomorphisms } \alpha\colon (\mathbf{Z}/3\mathbf{Z})^2_S \xrightarrow{\sim} E[n] \,\}.$$

An element of $[\Gamma(3)](E/S)$ is called a *(full) level 3 structure* on E. We are going to construct an elliptic curve E_3/M_3 which represents $[\Gamma(3)]$.

Let S be a $\mathbf{Z}[1/3]$-scheme, and let $(f\colon E \to S, \alpha)$ be an elliptic curve with level 3 structure. We define

$$P = \alpha(1,0), \quad Q = \alpha(0,1).$$

One can show (see Katz and Mazur [3], § 2.2) that locally on S, there exist functions x and y on E, regular outside O and with poles of order 2 and 3 along O, respectively, such that $y^2 - x^3$ has a pole of order at most 5 along O. Viewing $(x : y : 1)$ as a morphism $E \to \mathbf{P}^2_S$, we get (locally on S) an embedding $E \hookrightarrow \mathbf{P}^2_S$ given by a generalised Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

We claim that x and y can be chosen *uniquely* such that the following conditions hold (in addition to the condition that x and y satisfy a Weierstrass equation):

(1) $(x(P), y(P)) = (0,0)$;

(2) the tangent line to E at P in $\mathbf{P}^2_S$ (actually a family of lines over S) has equation $y = 0$;

(3) the tangent line to E at Q in $\mathbf{P}^2_S$ has equation $x + y = c$ for some $c \in \mathcal{O}_S(S)$.

First of all, we change x and y by subtracting the functions $x(P) \in \mathcal{O}_S(S)$ and $y(P) \in \mathcal{O}_S(S)$, respectively. This gives an equation of the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x$$

with P corresponding to $(0,0)$; note that a_6 vanishes because $(0,0)$ is on the curve. The tangent line to P is given by the equation

$$a_3y = a_4x,$$

and the fact that P is not annihilated by 2 in any fibre implies that the tangent line is nowhere parallel to the y-axis, from which it follows that a_3 is invertible. We can therefore change y by subtracting $(a_4/a_3)x$; this eliminates a_4, after which the fact that P is of order 3 (i.e. that the line $y = 0$ intersects E in $(0,0)$ with multiplicity 3) forces a_2 to vanish as well. Thus we get an equation of the form

$$y^2 + a_1xy + a_3y = x^3. \tag{$*$}$$

At this point, the conditions (1) and (2) are satisfied, and the only change of coordinates which preserves them is changing x by e^2 and y by e^3 for some element $e \in \mathcal{O}_S(S)^\times$. A calculation shows that the discriminant of the Weierstrass equation $(*)$ equals $(a_1^3 - 27a_3)a_3^3$, so that both a_3 and $a_1^3 - 27a_3$ must be invertible.

Let (u, v) be the coordinates of Q, the second point of order 3. Notice that u and v have non-zero value in all residue class fields of S: from $u = 0$ and $(*)$ we would get $v = 0$ or $v = -a_3$, hence $Q = \pm P$, and from $v = 0$ and $(*)$ we would get $u = 0$, hence $Q = P$. This implies that u and v are invertible.

The tangent line to E at Q is given by an equation of the form $y + bx = c$, since it is nowhere parallel to the y-axis (as Q is nowhere of order 2). The requirement that this tangent line, for which $x - u$ is a local parameter at (u, v), has a triple intersection point with E implies that

$$x^3 - (c - bx)^2 - a_1x(c - bx) - a_3(c - bx) = (x - u)^3.$$

Comparing coefficients of powers of x, we see that (u, v) is a point of order 3 on E if and only if

$$\begin{cases} 3u = b^2 - a_1b, \\ 3u^2 = 2bc - a_1c + a_3b, \\ u^3 = c^2 + a_3c. \end{cases}$$

Since u is invertible, the first equation shows that b is also invertible. We conclude that we can choose x and y uniquely (by dividing by b^2 and b^3, respectively) such that the equation for the tangent line becomes $x + y = c$, where now $c = u + v$ since Q lies on the line. The condition for Q to be a point of order 3 now reads

$$\begin{cases} 3u = 1 - a_1, \\ 3u^2 = 2(u+v) - a_1(u+v) + a_3, \\ u^3 = (u+v)^2 + a_3(u+v). \end{cases}$$

The first two equations are equivalent to

$$a_1 = 1 - 3u \quad \text{and} \quad a_3 = -3uv - u - v, \tag{$**$}$$

and the third can be rewritten as

$$u^3 = -3uv(u+v).$$

Since u is invertible, this last equation is equivalent to

$$u^2 + 3uv + 3v^2 = 0.$$

Finally, we note that the u and v, which have so far only been defined locally, glue together to elements of $\mathcal{O}_S^\times(S)$, since they are uniquely determined by (E, α).

Now let R_3 be the ring

$$R_3 = \mathbf{Z}[u,v]\left[\frac{1}{3}, \frac{1}{u}, \frac{1}{a_3}, \frac{1}{a_1^3 - 27a_3}\right] \Big/ (u^2 + 3uv + 3v^2),$$

where a_1 and a_3 defined by $(**)$, let M_3 be the affine scheme $\operatorname{Spec} R_3$, and let E_3 the elliptic curve over M_3 given by the equation $(*)$. The points

$$P_3 = (0,0), \quad Q_3 = (u,v)$$

are of order 3, and $Q_3 \neq \pm P_3$, so we get a level 3 structure

$$\alpha_3 \colon (\mathbf{Z}/3\mathbf{Z})^2_S \xrightarrow{\sim} E_3[3]$$

with $\alpha_3(1,0) = P_3$ and $\alpha_3(0,1) = Q_3$. We want to show that E_3/M_3 represents $[\Gamma(3)]$. Let E/S be any elliptic curve; we identify $h^{E_3/M_3}(E/S)$ with the set

$$\{(f,g) \mid f \colon S \to M_3 \text{ a morphism of schemes, } g \colon E \xrightarrow{\sim} f^*E_3\}.$$

For $f \colon E \to M_3$, we write

$$f^*\alpha_3 \colon (\mathbf{Z}/3\mathbf{Z})^2_S \xrightarrow{\sim} f^*(E_3[3])$$

for the pull-back of α_3 by f. Given $(f,g) \in h^{E_3/M_3}(E/S)$ we can then view $g^{-1} \circ f^*\alpha_3$ as an isomorphism from $(\mathbf{Z}/3\mathbf{Z})^2_S$ to $E[3]$. The map

$$\begin{aligned} \phi_{E/S} \colon h^{E_3/M_3}(E/S) &\longrightarrow [\Gamma(3)](E/S) \\ (f,g) &\longmapsto g^{-1} \circ f^*\alpha_3, \end{aligned}$$

is clearly functorial in E/S, and we have to prove that it is an isomorphism for all E/S. Given a level 3 structure

$$\alpha \colon (\mathbf{Z}/3\mathbf{Z})^2_S \xrightarrow{\sim} E[3]$$

on E, we define $f \colon S \to M_3$ by sending the elements $u, v \in R_3$ to the functions u and v on S associated to α via the construction above. Then both E and f^*E_3 are given by the Weierstrass equation $(*)$, so we get a canonical isomorphism $g \colon E \xrightarrow{\sim} f^*E_3$ for which $g \circ \alpha = f^*\alpha_3$ by the construction of u and v. We put $\phi_{E/S}^{-1}(\alpha) = (f,g)$; it is clear that this is the desired inverse of $\phi_{E/S}$.

5. Relatively representable moduli problems

Definition. We say a moduli problem $\mathcal{P}'$ is *relatively representable* if for every elliptic curve E/S the functor

$$\mathcal{P}' \circ F_{E/S} \colon \mathbf{Ell}_{E/S} \to \mathbf{Sets}$$

is representable.

Proposition 5.1. *Let $\mathcal{P}'$ be a moduli problem. The following are equivalent:*
(1) $\mathcal{P}'$ is relatively representable;
(2) for every representable moduli problem $\mathcal{P}$, the functor

$$\mathcal{P}' \circ F_{\mathcal{P}} \colon \mathbf{Ell}_{\mathcal{P}} \to \mathbf{Sets}$$

is representable;
(3) for every representable moduli problem $\mathcal{P}$, the simultaneous moduli problem

$$\begin{aligned} \mathcal{P} \times \mathcal{P}' \colon \mathbf{Ell} &\to \mathbf{Sets} \\ E/S &\mapsto \mathcal{P}(E/S) \times \mathcal{P}'(E/S) \end{aligned}$$

is representable.

Proof. The equivalence of (1) and (2) is clear from the definitions. For (2) $\iff$ (3), let $\mathcal{P}$ be a moduli problem represented by an elliptic curve E/S. If $\mathcal{P}' \circ F_{E/S} \colon \mathbf{Ell}_{E/S} \to \mathbf{Sets}$ is representable by an object

$$\begin{array}{ccc} E' & \longrightarrow & E \\ \downarrow & \square & \downarrow \\ S' & \longrightarrow & S \end{array}$$

then the object E'/S' of $\mathbf{Ell}$ represents $\mathcal{P} \times \mathcal{P}'$. Conversely, if $\mathcal{P} \times \mathcal{P}'$ is representable by an elliptic curve E'/S', then Yoneda's lemma gives a morphism $E'/S' \to E/S$ corresponding to the projection $\mathcal{P} \times \mathcal{P}' \to \mathcal{P}$; viewing this morphism as an object of $\mathbf{Ell}_{E/S}$, we get a representing object of $\mathcal{P}' \circ F_{E/S}$. ☐

Proposition 5.2. *Every representable moduli problem is relatively representable.*

Proof. Let $\mathcal{P}$ be a representable moduli problem. By Fact 1.1, $\mathcal{P} \times \mathcal{P}'$ is representable for every representable moduli problem $\mathcal{P}'$, so $\mathcal{P}$ is relatively representable by the previous proposition. ☐

Notation. If $\mathcal{P}$ is a representable moduli problem, we write $E_{\mathcal{P}} \to M_{\mathcal{P}}$ for the representing object in $\mathbf{Ell}$. If $\mathcal{P}$ is a relatively representable moduli problem and $E \to S$ is any elliptic curve, we write

$$\begin{array}{ccc} E_{\mathcal{P};E/S} & \longrightarrow & E \\ \downarrow & \square & \downarrow \\ M_{\mathcal{P};E/S} & \longrightarrow & S \end{array}$$

for the representing object in $\mathbf{Ell}_{E/S}$.

Let $\mathcal{P}$ be a representable moduli problem. The scheme $M_{\mathcal{P}}$ is called the *(fine) moduli scheme* associated to $\mathcal{P}$, and the elliptic curve $E_{\mathcal{P}}$ is called the *universal elliptic curve* over $M_{\mathcal{P}}$. If $\mathcal{P}$ is a relatively representable moduli problem and E/S is any elliptic curve, then the moduli problem $\mathcal{P} \times h^{E/S}$ is representable and $M_{\mathcal{P};E/S}$ is the moduli scheme associated to $\mathcal{P} \times h^{E/S}$.

Exercise. Let $\mathcal{P}$ be a representable moduli problem. Show that the scheme $M_{\mathcal{P}}$ represents the functor from $\mathbf{Sch}$ to $\mathbf{Sets}$ which sends a scheme S to the set of isomorphism classes of pairs $(E/S, \alpha)$ with E/S an elliptic curve and $\alpha \in \mathcal{P}(E/S)$ a $\mathcal{P}$-structure on E/S.

6. Rigidity and representability

Definition. Let $\mathcal{P}$ be a moduli problem. For every elliptic curve $f\colon E \to S$, the group

$$\mathrm{Aut}_S(E) = \{g\colon E \xrightarrow{\sim} E \mid fg = f\}$$

acts from the right on the set $\mathcal{P}(E/S)$ by functoriality of $\mathcal{P}$. We say that $\mathcal{P}$ is *rigid* if $\mathrm{Aut}_S(E)$ acts freely on $\mathcal{P}(E/S)$, i.e. if for every elliptic curve E/S and every $\alpha \in \mathcal{P}(E/S)$, the only element of $\mathrm{Aut}_S(E)$ fixing α is the identity.

Definition. If $\mathcal{P}$ is relatively representable, we say that $\mathcal{P}$ is *affine* (resp. *étale*, *finite*, or some other property of morphisms of schemes) if for every elliptic curve E/S, the object $M_{\mathcal{P};E/S}$ is affine (resp. étale, finite, ...) over S.

An extremely useful criterion for representability is the following theorem.

Theorem 6.1. *Let $\mathcal{P}$ be a relatively representable and affine moduli problem for elliptic curves over $\mathbf{Z}$-schemes. Then $\mathcal{P}$ is representable if and only if $\mathcal{P}$ is rigid. In this case, the moduli scheme $M_{\mathcal{P}}$ is affine, and if in addition $\mathcal{P}$ is étale, then $M_{\mathcal{P}}$ is a smooth curve over $\mathbf{Z}$.*

Proof. See Katz and Mazur [3], § 4.7.

Exercise. Let $\mathcal{P}$ be a rigid moduli problem, and assume that the functor from **Sch** to **Sets** which sends a scheme S to the set of isomorphism classes of pairs $(E/S, \alpha)$, with E/S an elliptic curve and $\alpha \in \mathcal{P}(E/S)$ a $\mathcal{P}$-structure, is representable by a scheme M. Prove that there exists an elliptic curve E/M (a so-called *universal elliptic curve* for the moduli problem $\mathcal{P}$) such that the object E/M of **Ell** represents $\mathcal{P}$.

7. The moduli problems $\Gamma(n)$, $\Gamma_1(n)$ and $\Gamma_0(n)$

The moduli problems which are the most important in practice are those which classify elliptic curves with “extra structure” attached to the n-torsion, where n is some positive integer. The “extra structure” in these problems is known as *level n structure*. Specifically, we have the following moduli problems on $\mathbf{Z}[1/n]$-schemes (see § 3):

$$\begin{aligned}
[\Gamma(n)]\colon E/S &\longmapsto \{\,\text{isomorphisms } (\mathbf{Z}/n\mathbf{Z})_S^2 \xrightarrow{\sim} E[n]\,\};\\
[\Gamma_1(n)]\colon E/S &\longmapsto \{\,\text{embeddings of group schemes } (\mathbf{Z}/n\mathbf{Z})_S \hookrightarrow E[n]\,\};\\
[\Gamma_0(n)]\colon E/S &\longmapsto \{\,\text{subgroup schemes of } E[n] \text{ locally isomorphic to } \mathbf{Z}/n\mathbf{Z}\,\}.
\end{aligned}$$

In the last line, ‘locally’ means *locally for the étale topology on S*: a subgroup scheme H of $E[n]$ is locally isomorphic to $\mathbf{Z}/n\mathbf{Z}$ if and only if there exists a surjective étale morphism $S' \to S$ such that $H \times_S S'$ is isomorphic to the constant group scheme $\mathbf{Z}/n\mathbf{Z}$ over S'.

The fundamental results about these moduli problems are as follows:

Theorem 7.1. *For all $n \geq 1$, the moduli problems $[\Gamma(n)]$, $[\Gamma_1(n)]$, $[\Gamma_0(n)]$ are relatively representable and finite étale. Moreover, $[\Gamma(n)]$ is representable for $n \geq 3$, and its moduli scheme is a smooth affine curve over $\mathrm{Spec}\,\mathbf{Z}[1/n]$. The same holds for $[\Gamma_1(n)]$ with $n \geq 4$.*

Proof. According to Katz and Mazur [3], Theorem 3.7.1, each of the above moduli problems is relatively representable and finite étale. Furthermore, $\Gamma(n)$ for $n \geq 3$ and $\Gamma_1(n)$ for $n \geq 4$ are rigid by Corollaries 2.7.2 and 2.7.4 of [3], respectively, so Theorem 6.1 (which remains true if $\mathbf{Z}$ is replaced by $\mathbf{Z}[1/n]$) implies that they are representable by smooth affine curves over $\mathrm{Spec}\,\mathbf{Z}[1/n]$. □

Exercise. Show that the moduli problem $[\Gamma_0(n)]$ is not rigid for any $n \geq 1$, and conclude that it is not representable (cf. Theorem 6.1).

8. Compactification

The moduli schemes resulting from these moduli problems, known as *modular curves*, are not proper over $\operatorname{Spec}\mathbf{Z}$. This is a problem “in two directions”: the curves have only been defined over the open subset $\operatorname{Spec}\mathbf{Z}[1/n]$ of $\operatorname{Spec}\mathbf{Z}$, and moreover they are affine. Both observations pose an obstacle in the way of developing a good theory of modular forms (although the requirement that n be invertible mainly becomes a problem for the arithmetic theory). One way to get a proper curve over $\operatorname{Spec}\mathbf{Z}$ out of an affine modular curve Y over $\operatorname{Spec}\mathbf{Z}[1/n]$ is by viewing the j-invariant as a morphism

$$j\colon Y \to \mathbf{A}^1_{\mathbf{Z}[1/n]}$$

and by considering the normalisation of Y over the proper $\mathbf{Z}$-scheme $\mathbf{P}^1_{\mathbf{Z}}$.

The problem with this approach is that it leads to rather messy computations because the interpretation of the curve as a moduli scheme is lost. There are two things that must be generalised in order to ‘compactify’ the affine modular curves in a ‘modular’ way:

(1) Together with elliptic curves in the usual sense, consider *generalised elliptic curves*, which are either elliptic curves or polygons of projective lines. This is the approach taken by Deligne and Rapoport [2]; Katz and Mazur [3] use the normalisation over the ‘compactified’ j-line $\mathbf{P}^1_{\mathbf{Z}}$.

(2) Allow so-called *Drinfeld level structures* as well as the ordinary level structures defined above. This is done in [3], whereas the technique of normalisation is used in [2].

It is harder to do both generalisations simultaneously; there is a recent article by Conrad [1] in which the theory of moduli of generalised elliptic curves with Drinfeld structures is developed.

References

[1] B. D. Conrad, Arithmetic moduli of generalized elliptic curves. *J. Inst. Math. Jussieu* **6** (2007), no. 2, 209–278.

[2] P. Deligne and M. Rapoport, Les schémas de modules de courbes elliptiques. In: P. Deligne and W. Kuyk (eds.), *Modular Functions of One Variable II* (Proc. Internat. Summer School, Univ. Antwerp, 1972), 143–316. Springer-Verlag, Berlin/Heidelberg, 1973.

[3] N. M. Katz and B. Mazur, *Arithmetic Moduli of Elliptic Curves.* Ann. Math. Studies **108**. Princeton University Press, Princeton, NJ, 1985.