25.6.2024

Construction of modular curves

We have discussed that quotients $\Gamma\backslash\mathbb{H}$, $\Gamma \subset SL_2(\mathbb{Z})$ a congruence subgroup, parametrize elliptic curves E (with additional structure, such as an isomorphism $E[N] \xrightarrow{\sim} (\mathbb{Z}/N)^2$) up to isomorphism, and are (the analytifications) of quasi-projective algebraic curves $/\mathbb{C}$.

We will now discuss a way to construct such "modular curves" using algebraic techniques.

This makes it easier to use algebraic tools to study these curves, but more importantly allows to construct modular curves over (finite extensions of) $\mathbb{Q}$ or even over (open subschemes of) $\operatorname{Spec}\mathbb{Z}$.

There are several possible approaches:

- "classical" (study the fields of rational fcts of $t^{1/N}$ and find "models" over $\mathbb{Q}$)

- Igusa's approach: consider ell. curves + add'l data which allows to describe the ell. curve by a uniquely determined Weierstrass equation (of some form)

(this is the path we will take in this class)

- geometric invariant theory

(see next page)

- Artin's criteria for representability of a functor by an algebraic space (or algebraic stack)

Sketch: Construction of moduli spaces via Geometric Invariant Theory (GIT)

Reference
[GIT] Mumford, Fogarty, Kirwan: Geometric Invariant Theory, Springer, Ch. 7, Thm 7.9

Fix $g \in \mathbb{Z}_{\geq 1}$, $n \in \mathbb{Z}$, $n \geq 3$.

Goal: Construct scheme $\mathcal{A}_g$ representing the functor $(Sch/\mathbb{Z}[\frac{1}{n}])^{op} \to (Sets)$,

$S \mapsto \{(A, \lambda, \eta)$; A/S abelian scheme of rel. dim g,
$\lambda : A \xrightarrow{\sim} A^\vee$ principal polarization,
$\eta : A[n] \xrightarrow{\sim} (\mathbb{Z}/n\mathbb{Z})^{2g}\} / \cong$.

$E^\vee \xrightarrow{id} E^\vee \rightsquigarrow$ l.b. on $E \times E^\vee$ flam. by $0/E^\vee$

Lemma Let $(A, \lambda, \eta)/S$ as above, and let $\mathcal{L}(\lambda)$ be the pullback of the universal line bundle $\mathcal{P}$ on $A \times A^\vee$ along $A \xrightarrow{(id, \lambda)} A \times A^\vee$ (cf [GIT] Ch. 6). Then $\mathcal{L}(\lambda)$ is ample, $\mathcal{L}(\lambda)^{\otimes 3}$ is very ample and (writing $A \xrightarrow{\pi} S$) $\pi_*(\mathcal{L}(\lambda)^{\otimes 3})$ is a loc. free $\mathcal{O}_S$-module of rank 6^g.

(For $g=1$ and λ the canon. polarization of the ell. c. A, $\mathcal{L}(\lambda) = \mathcal{O}(2[0])$, so we know the lemma in this case.)

By the lemma, obtain canonical closed embedding

$$A \hookrightarrow \mathbb{P}(\pi_*(\mathcal{L}(\lambda))^{\otimes 3}) \leftarrow \text{projective bundle } /S$$

Now the construction of A_g proceeds in 2 steps:

Step 1 Construct a scheme $\mathcal{H}_g$ representing the functor

$$S \mapsto \{(A, \lambda, \eta, \varphi : \mathbb{P}(\pi_*(\mathcal{L}(\lambda)^{\otimes 3})) \xrightarrow{\sim} \mathbb{P}_S^{6g-1}\}$$

(A, λ, η: as for $\mathcal{A}_g$)

(use the Hilbert scheme parametrizing closed subschemes of $\mathbb{P}^{6g-1}$, see [GIT] 7.2).

$$\mathrm{Aut}(\mathbb{P}^{6g-1}) = PGL_{6g}$$

Step 2 Then $PGL_{6g} \curvearrowright \mathcal{H}_g$ by $g \cdot (A, \lambda, \eta, \varphi) := (A, \lambda, \eta, g \circ \varphi)$.

Since any two isom. φ differ by an element of PGL_{6g}, we expect that

$A_g \leftrightarrow$ quotient of $\mathcal{H}_g$ by the above PGL_{6g}-action.

Using GIT, can construct quotient $PGL_{g^2} \backslash \mathcal{H}_g$, and it follows that the scheme $PGL_{g^2} \backslash \mathcal{H}_g$ represents the functor $\mathcal{A}_g$.

(More precisely, to carry this out, consider the

PGL - equivariant morphism

$$\mathcal{H}_g \longrightarrow \left(\mathbb{P}^{g^2-1}\right)^{n^{2g}}$$

$(A, \lambda, \eta, \mathcal{C}) \mapsto$ image of the pts in $A[n]$ under $A[n] \subset A \hookrightarrow \mathbb{P}^{g^2-1}$

[To fix an order for the points in $A[n]$ we use the level structure (and an order of $(\mathbb{Z}/n)^{2g}$ that we fix).]

One shows that the image of $\mathcal{H}_g$ lies inside "stable locus" in the sense of GIT w.r.t. the diagonal action of PGL and the canonically linearized line bundle $\mathcal{O}(1) \boxtimes \cdots \boxtimes \mathcal{O}(1)$.

By GIT, then quotient $PGL_{g^2} \backslash \left(\mathbb{P}^{g^2-1}\right)^{n^{2g}}$, stable

and using "faithfully flat descent" one obtains the quotient $\mathcal{H}_g \to PGL_{g^2} \backslash \mathcal{H}_g$.)

What are we looking for?

"fine moduli space" (scheme representing a given functor $F: (Sch/S)^{op} \to (Sets)$)

If no fine moduli space exists for a given functor $F: (Sch/S)^{op} \to (Sets)$, one can still look for a coarse moduli space, i.e., a scheme X/S together with a morphism $F \to Hom(-, X)$ a functor $(Sch/S)^{op} \to (Sets)$ s.t.

① for all S-schemes T

and all morphisms $F \to Hom(-, T)$ factors as

$F \to Hom(-, X) \to Hom(-, T)$ for a unique $X \to T$,

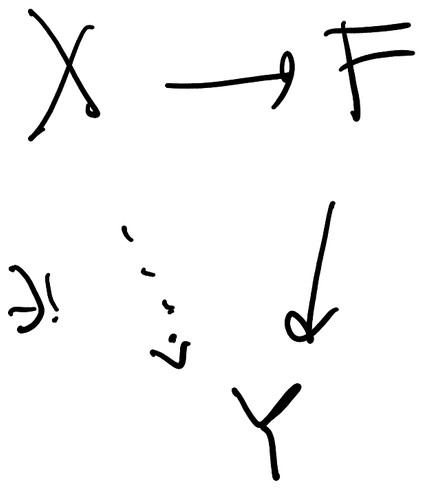
② for every alg. closed field k and morphism $Spec\, k \to S$, $F(Spec\, k) \to Hom(Spec\, k, X)$ is bijective.

Rmks (1) A coarse moduli space, if it exists, is uniquely determined.

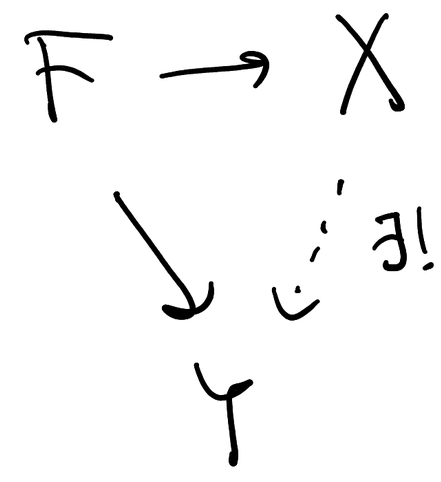
(2) If F is repres. by a scheme X, then X is a coarse moduli space for F.

Remark The universal properties of a repres. functor (fine moduli space) and coarse moduli space are "dual to each other":

functor F represented by X:



$F \to X$ coarse moduli space for F:



Example Consider the "naive" moduli functor

$$\mathcal{M} : (Sch)^{op} \to (Sets), \quad S \mapsto \{E/S \text{ rel. ell. curve}\}/\cong.$$

Then $\mathcal{M}(\mathbb{Q}) \to \mathcal{M}(\bar{\mathbb{Q}})$ is not injective (consider quadratic twists as in Problem 26).

Thus $\mathcal{M}$ is **not** representable.

(I) Theorem The functor

$$\widetilde{\mathcal{M}} : \left(\mathrm{Sch}/\mathbb{Z}[\tfrac{1}{6}]\right)^{\wedge} \longrightarrow (\mathrm{Sets})$$

$$S \longmapsto \left\{ (E, \omega)\,;\quad E/S \text{ rel ell. c.},\ \omega \text{ basis } \eta\ \omega_{E/S} \right\}/\cong$$

is representable by

$$\widetilde{M} := \mathrm{Spec}\ \mathbb{Z}\left[\tfrac{1}{6}, a, b, \Delta^{-1}\right], \qquad \Delta = 4a^3 + 27b^2$$

with universal object $(\mathcal{E}, \omega) \in \widetilde{\mathcal{M}}(\widetilde{M})$ with

$$\mathcal{E} = V_+\left(Y^2Z - X^3 - aXZ^2 - bZ^3\right) \subset \mathbb{P}^2_{\widetilde{M}}$$

$$\omega = -\frac{dx}{2y} \overset{\nabla}{=} -\frac{dy}{3x^2+a}$$

$(\mathrm{mod}\ (y))$ — $d(y^2 - x^3 - ax - b) = 0$ $(\mathrm{mod}\ (3x^2+a))$

It is easy to check that the universal object is of the desired form (i.e. ω is a basis of $\omega_{\mathcal{E}/\widetilde{M}}$).

This property is preserved under pullback, so we obtain

$\widetilde{M} \to \widetilde{\mathcal{M}}$. Want to show that this is an iso.

To do so, we construct inverse map $\tilde{\mathcal{M}} \to \tilde{\mathcal{N}}$.
The key for this is:

Lemma Let S be a $\mathbb{Z}[\frac{1}{6}]$-scheme,
$E \xrightarrow{f} S$ an elliptic curve s.t. $\omega_{E/S}$ is free,
ω a basis of $\omega_{E/S}$.

Then there is a unique choice of
$x \in \Gamma(S, f_* \mathcal{O}_E(2[0]))$, $y \in \Gamma(S, f_* \mathcal{O}_E(3[0]))$
such that the corresp Weierstrass equation
(cf. the previous chapter) has the form

$$y^2 = x^3 + ax + b, \qquad a, b \in \Gamma(S, \mathcal{O}_S)$$

(unique since they are uniquely det. by x, y)

And that $\omega = -\frac{dx}{2y}$.

Given the Lemma, we obtain $\mathcal{M} \to \mathcal{N}$

$$\Big((E, \omega) \in \tilde{\mathcal{M}}(S) \xrightarrow[\text{Lemma}]{} a, b \in \Gamma(S, \mathcal{O}_S) \rightsquigarrow S \to \tilde{\mathcal{N}} \Big),$$

and the compositions $\underbrace{\tilde{\mathcal{M}} \to \tilde{\mathcal{N}} \to \tilde{\mathcal{M}}}$ and $\underbrace{\tilde{\mathcal{N}} \to \tilde{\mathcal{M}} \to \tilde{\mathcal{N}}}$ are $= \mathrm{id}$.

clear "for E", see below "for ω" ↗

clear from uniqueness statement in the Lemma ↗

Proof of the Lemma

It is enough to consider the case that S is affine (since x, y, a, b are unique, then can use gluing to handle the general case).

Alternatively, to prove the theorem it is sufficient to

- prove the Lemma for S affine
- prove that $\mathrm{Aut}(E, \omega) = \{\mathrm{id}\}$ for (E, ω) as in the Lemma

(cf. Problem 47). □

We now use the results of the previous chapter: There we have seen that E has a Weierstraß equation description, induced by a choice of basis $1, x, y$ of $\mathbb{O}(3[0])$ as above.

in particular:

- $x \longmapsto \omega^{-2}$
  $\Uparrow$
  $\mathcal{O}(2[0]) \twoheadrightarrow \mathcal{O}(2[0])/\mathcal{O}([0]) \cong \omega_{E/S}^{\otimes -2}$
- $y \longmapsto \omega^{-3}$

and then x, y are uniquely determined up to

$$\circledast \quad \begin{aligned} x &\longmapsto x + r =: x', \\ y &\longmapsto y + sx + t =: y', \end{aligned} \qquad r, s, t \in \Gamma(S, \mathcal{O}_S)$$

A coordinate change $\circledast$ changes the coefficients of our Weierstraß equation from $a_1, a_2, \dots, a_6$ to

$$\begin{aligned} a_1 &= a_1' + 2s \\ a_2 &= a_2' - s a_1' + 3r - s^2 \\ a_3 &= a_3' + r a_1' + 2t \\ &\vdots \end{aligned}$$

$\rightsquigarrow$ there exist unique r, s, t such that

$$a_1' = a_2' = a_3' = 0.$$

This concludes the proof of the lemma.

As explained above, to conclude the proof of the theorem, it remains to show that for this choice of $1, x, y$, the given ω has the form $-\frac{dx}{2y}$.

$$\text{“}\frac{x \bmod \mathcal{O}_S}{y \bmod \mathcal{O}_S(2[O])}\text{”}$$

- ω and $-\frac{dx}{2y} \in \Gamma(S, \omega_{E/S}) = \Gamma(E, \Omega^1_{E/S})$ each are a basis of $\omega_{E/S}$, so they differ by an element of $\Gamma(S, \mathcal{O}_S)^\times$.

To show this elt $\bar{\omega} = 1$, enough to show that their restrictions to $e(S)$ coincide.

- Locally on E, we have $I = (t)$, and we may write $x = \frac{f}{t^2}$, $y = \frac{g}{t^3}$, $f, g \in \Gamma(U, \mathcal{O}_E)$, units at $e(S)$.

$$\rightsquigarrow \quad \omega = \frac{x}{y} \bmod I^2 = \frac{f}{g} \cdot t \bmod I^2 = d\left(\frac{f}{g} \cdot t\right) \overset{\circledast}{=} \frac{f}{g}(e) \cdot dt$$

$$\begin{array}{ccc} \cap & & \cap \\ \omega_{E/S} & = & I/I^2 \end{array} \qquad I/I^2 \xrightarrow{\sim} \omega_{E/S} \xrightarrow{\sim} e^* \Omega^1_{E/S}, \quad \varphi \longmapsto e^*(d\varphi)$$

On the other hand,

$$-\frac{dx}{2y} = -\frac{t^2 df - 2tf\,dt}{t^4} \cdot \frac{t^3}{2g} = \frac{f}{g}\,dt - \frac{t}{2g}\,df,$$

so $e^*\left(-\frac{dx}{2y}\right) = \left(\frac{f}{g}\right)(e)\,dt$

$\circledast$ $e^* d\left(\frac{f}{g} t\right) = \underbrace{e^*\left(\frac{f}{g}\right)}_{\left(\frac{f}{g}\right)(e)} \cdot dt + \underbrace{e^*(t)}_{t(e) = 0} \cdot d\left(\frac{f}{g}\right)$

Remark Then exist schemes S (can be chosen affine and $/\mathbb{C}$) and ell. curves E/S such that $\omega_{E/S}$ is (only locally free but) not free.

In fact, let $S/\mathbb{C}$ be a modular curve, i.e. $S^{an} \cong \Gamma\backslash\mathcal{H}$ for a suff. small congruence subgroup $\Gamma \subset SL_2(\mathbb{Z})$

Then the functor of points of S can be described (at least for suitable Γ) as

$$S(T) = \left\{ (E/T \text{ ell. curve} + \text{add'l data}) \right\} / \cong$$
("level structure")

$\rightsquigarrow$ here universal elliptic curve E/S

The Kodaira-Spencer isomorphism then gives an isomorphism $\omega_{E/S}^{\otimes 2} \cong \Omega^1_{S/\mathbb{C}}$.

Since the RHS is typically non-trivial (it is related to modular forms of weight 2 and level Γ) we obtain examples where $\omega_{E/S}^{\otimes 2}$ and a fortiori $\omega_{E/S}$ is non-trivial.

Remarks
- note that $\tilde{\mathcal{M}}$ has relative dimension 2 over $\mathbb{Z}$ (so it is not a relative curve and does not deserve the name "moduli curve").

- Coarse moduli space.

Recall $\mathcal{M} : S \mapsto \{ E/S \text{ ell. curve} \}/\cong$
(consider this here as a functor $(\mathrm{Sch}/\mathbb{Z}[\frac{1}{6}])^{op} \to (\mathrm{Sets})$).

Have forgetful morphism $\tilde{\mathcal{M}} \to \mathcal{M}$ of functors.

Fibers are empty or have simply transitive action by $\Gamma(S, \mathcal{O}_S)^\times$ (if $(E,\omega) \in \tilde{\mathcal{M}}(S)$, then any two basis vectors differ by unique elem. of $\Gamma(S,\mathcal{O}_S)^\times$

On the other hand, can form the quotient of $\tilde{\mathcal{M}}$ by the $\mathbb{G}_m$-action $u \cdot (E,\omega) := (E, u\omega)$
as a scheme: $\tilde{\mathcal{M}}/\mathbb{G}_m = \mathrm{Spec}\, \mathbb{Z}[\frac{1}{6}, a, b, \Delta^{-1}]^{\mathbb{G}_m}$

[Easy to check that this satisfies the "classical" universal property of the quotient in the category of affine schemes. One checks that the same holds in category of all schemes. ∎

Scaling u by u changes a by u^4,

b by u^6

$\rightsquigarrow$ the ring $\mathbb{Z}[\frac{1}{6}, a, b, \Delta^{-1}]^{\mathbb{G}_m}$ of invariants is the subring of $\mathbb{Z}[\frac{1}{6}, a, b, \Delta^{-1}]$ consisting of all elements $\frac{f(a,b)}{\Delta^i}$ s.t. $\frac{f(u^4a, u^6b)}{u^{12}\cdot\Delta^i} = \frac{f(a,b)}{\Delta^i}$

(in $\mathbb{Z}[\frac{1}{6}, a, b, \Delta^{-1}, u, u^{-1}]$)

$\Leftrightarrow$ $u^{-12i} f(u^4a, u^6b) = f(a,b)$

E.g. $\frac{a^3}{\Delta}$, $\frac{b^2}{\Delta}$ have this property, and one checks that these elements generate the ring $\mathbb{Z}[\frac{1}{6}, a, b, \Delta^{-1}]^{\mathbb{G}_m}$

Since $\frac{4a^3}{\Delta} + \frac{27b^2}{\Delta} = 1$, we have $\frac{b^2}{\Delta} \in \mathbb{Z}[\frac{1}{6}, \frac{a^3}{\Delta}]$

$\rightsquigarrow$ $\mathbb{Z}[\frac{1}{6}, a, b, \Delta^{-1}]^{\mathbb{G}_m} = \mathbb{Z}[\frac{1}{6}, \underbrace{\frac{a^3}{\Delta}}_{\| \; j}] = \mathbb{Z}[\frac{1}{6}, j]$

polynomial ring in one variable j

Note that (up to a unit in $\mathbb{Z}[\frac{1}{6}]$)

$\frac{a^3}{\Delta}$ is the j-invariant of the ell. curve $y^2 = x^3 + ax + b$ that we have discussed before.

This gives an intrinsic definition of the j-invariant of an elliptic curve (up to units in $\mathbb{Z}[\frac{1}{6}]$) and shows that the map $\tilde{\mathcal{M}} \to \tilde{\mathcal{M}}/\mathbb{G}_m$ can be identified with $\tilde{\mathcal{M}} \to \mathbb{A}^1_{\mathbb{Z}[\frac{1}{6}]}$.

$$(E,\omega) \longmapsto j(E)$$

Since the image of (E,ω) in $\tilde{\mathcal{M}}/\mathbb{G}_m = \mathbb{A}^1_{\mathbb{Z}[\frac{1}{6}]}$ is independent of ω, we obtain a commutative diagram of morphisms of functors

$$\begin{array}{ccc} \tilde{\mathcal{M}} & \longrightarrow & \mathcal{M} \\ & \searrow \quad \swarrow & \\ & \mathbb{A}^1_{\mathbb{Z}[\frac{1}{6}]} & \end{array}$$

Proposition Via the morphism $\mathcal{M} \to \mathbb{A}^1_{\mathbb{Z}[\frac{1}{6}]}$, $\mathbb{A}^1_{\mathbb{Z}[\frac{1}{6}]}$ is a coarse moduli space for $\mathcal{M}$.

Idea of proof • Know already: $\mathcal{M}(k) = \{\text{ell. curves}/k\} \to \mathbb{A}^1(k)$ for k alg. closed field

• Given $\mathcal{M} \to \mathcal{Y}$, consider $\tilde{\mathcal{M}} \to \mathcal{M} \to \mathcal{Y}$ and show it factors through $\tilde{\mathcal{M}}/\mathbb{G}_m$. Then check that $\begin{array}{ccc} \mathcal{M} & \to & \mathcal{Y} \\ \downarrow & \nearrow & \\ \mathbb{A}^1_{\mathbb{Z}[\frac{1}{6}]} & & \end{array}$ commutes.

Remark Another issue we would like to resolve is the restriction to schemes S on which 6 is invertible.

Remark The theorem implies that for S a $\mathbb{Z}[\frac{1}{6}]$-scheme, an elliptic curve E/S admits a Weierstraß equation if and only if $\omega_{E/S}$ is free.

Remark Let S be a $\mathbb{F}_2$-scheme, E/S ell.c., ω a basis of $\omega_{E/S}$. Then $[-1]_E$ induces a non-trivial automorphism of (E, ω) (since $-\omega = \omega$). Thus the method cannot extend to characteristic 2.

(I) The Legendre family (Assume 2 invertible)

Let S be a $\mathbb{Z}[\frac{1}{2}]$-scheme, E/S an ell. curve

s.t. $\omega_{E/S}$ free with basis ω.

⟶ Weierstrass eqn for E "in x, y",

as above

where x unique up to $x \mapsto x+r$

y unique if we require that

$$a_1 = a_3 = 0$$

$$\rightsquigarrow \quad y^2 = x^3 + a_2 x^2 + a_4 x + a_6,$$

and similarly as before, $\omega = -\frac{dx}{2y}$.

The automorphism $[-1]_E$ then has the form

$(x,y) \mapsto (x,-y)$

[The line $L \subset \mathbb{P}^2$ through $(x,y), (x,-y)$ intersects E in $(x,y), (x,-y), 0 = (0:1:0)$ $\quad (L = V_+(X - xZ))$

Viewing L as divisor, $\mathcal{O}(L) = \mathcal{O}(1)$, so

$$\mathcal{O}\big([x,y] - [0] + [x,-y] - [0] + [0] - [0]\big)$$

$$= \mathcal{O}(1)|_E \otimes \mathcal{O}(3[0])^{-1} = \mathcal{O}_E \rightsquigarrow (x,y) + (x,-y) = 0.$$]

$\rightsquigarrow$ $E[2] \overset{\text{"}}{=}$ neutral elem η E
+ the three zeros η $x^3 + a_2x^2 + a_4x + a_6$.

Now for 2-torsion pts $P_2, Q_2 \in E(S)$, disjoint from O and from each other (after an étale base change, if necessary).

(Then the third pt, R_2 say, is equal to $P_2 + Q_2$ since $E[2] \cong (\mathbb{Z}/2)^2$.)

Then there is a unique r s.t. replacing x by $x + r$ ensures that $x(P_2) = 0$.

Since P_2, Q_2 disjoint from each other, $x(Q_2)$ invertible.

Thus, there is a unique (up to ± 1) scalar multiple η of x st. in addition $x(Q_2) = 1$.

Replacing x by $u^{-2}x$
y by $u^{-3}y$.

Again a finite étale base change may be required to "extract a square root η $x(Q_2)$".

Theorem The functor

$$\mathcal{M}_{\text{Legendre}} : \left(\mathcal{M}_{/\mathbb{Z}[\frac{1}{2}]}\right)^{op} \longrightarrow (\text{Sets})$$

$$S \longmapsto \left\{ (E, \omega, P_2, Q_2) \;;\; E/S \text{ ell. curve},\ \omega \text{ basis of } \omega_{E/S},\ P_2, Q_2 \in E[2](S) \smallsetminus \{0\} \right\}$$

(i.e. P_2, Q_2 disjoint from 0)

$$\text{s.t. } x(P_2) = 0,\ x(Q_2) = 1 \qquad \Big/ \simeq$$

is representable by

$$\operatorname{Spec} \mathbb{Z}\left[\tfrac{1}{2}, \lambda, \frac{1}{\lambda(\lambda-1)}\right]$$ with universal object

$$\mathcal{E}: \quad y^2 = x(x-1)(x-\lambda)$$

$$\omega = -\frac{dx}{2y}, \qquad P_2 = (0,0), \quad Q_2 = (1,0).$$

(Note that in this case we obtain a "modular curve", i.e. a scheme of rel. dim. 1 over $\mathbb{Z}$.)

Naive level 3 (3 invertible)

2.7.2024

Theorem The functor

$$M_3 : (Sch/\mathbb{Z}[\tfrac{1}{3}])^{op} \longrightarrow (Sets),$$
$$S \longmapsto \{(E, P_3, Q_3);$$

E/S elliptic curve

$P_3, Q_3 \in E[3](S)$

disjoint from 0 and

P_3 disjoint from $Q_3, -Q_3$ $\}/\simeq$

$(\mathbb{Z}/N)^2 \xrightarrow{\sim} E[N]$ ⟷

$(1,0) \longmapsto P_3$

$(0,1) \longmapsto Q_3$

is representable by

$$\operatorname{Spec} \mathbb{Z}[\tfrac{1}{3}, B, C, (a_1^3 - 27 a_3)a_3 C)^{-1}] / (B^3 - (B+C)^3)$$

where $a_1 = 3C - 1$, $a_3 = -3C^2 - B - 3BC$

with universal object

$$E: y^2 + a_1 xy + a_3 y = x^3$$

$$P_3 = (0,0), \quad Q_3 = (C, B+C).$$

Proof. As before locally on S we pick a basis of $\Omega_{E/S}$.

$\rightsquigarrow$ Obtain x, y where we choose the unique x s.t. $a_2 = 0$, so that we get a Weierstraß equation for E of the form $y^2 + a_1 xy + a_3 y = x^3 + a_4 x + a_6$.

Since $3P_3 = 0$, we have $\mathcal{O}_E(3([P_3]-[O])) \simeq \mathcal{O}_E$

or in other words $\mathcal{O}(3[P_3]) \simeq \mathcal{O}(3[O])$.

So there exist unique $a, b \in \Gamma(S, \mathcal{O}_S)$ s.t.

$$\operatorname{div}(\underbrace{y + ax + b}_{\in \Gamma(\mathcal{O}(3[O]))}) = 3[P_3]$$

Replacing y by $y + ax + b$ we obtain coordinates x, y with $y(P_3) = 0$ and a Weierstraß eqn of the form

$$y^3 + a_1 xy + a_3 y = \underbrace{(x-c)^3}_{\text{for } y=0 \text{ must have triple zero}} = x^3 \quad (a_2 = 0 \text{ implies } c = 0)$$

and it follows that $x(P_3) = 0$.

The above Weierstraß equation defines a smooth curve if and only if $(a_1^3 - 27a_3)\, a_3$ is invertible.

One computes that $-P_3 = (0, -a_3)$.

Now $Q_3 \in E(S)$ has order 3 and is disjoint from P_3 and $-P_3$.

Similarly as above, we find unique A, B s.t. $\operatorname{div}(y - Ax - B) = 3[Q_3]$.

Claim A is invertible.

Proof of claim We can check this on residue class fields, so WLOG $S = \operatorname{Spec} k$, k a field, $\operatorname{char}(k) \neq 3$.

Suppose $A = 0$, i.e., $\operatorname{div}(y - B) = 3[Q_3]$.

We have (setting $y = B$): $x^3 - (B^2 + a_1 x B + a_3 B) = (x - x(Q_3))^3$

and comparing the coefficients of x^2 we see that $x(Q_3) = 0$,

so $Q_3 = \pm P_3$, a contradiction. ∎

Thus there is a unique choice for u s.t. $A = 1$.

(Note that replacing u by u' means

replacing $y - Ax - B$ by

$u'^{-3} y - u'^{-2} A x - B = u'^{-3}(y - uAx - u^3 B)$, so set $u = A^{-1}$.)

Then $y = x + B$ intersects E with multiplicity 3,

so with $y = x + B$, $C = x(Q_3)$: $x^3 - \left((x+B)^2 + (a_1 x + a_3)(x+B)\right) = (x - C)^3$,

→ compare coefficients

$$3C = 1 + a_1 \qquad \text{I}$$

$$-3C^2 = 2B + a_1 B + a_3 \qquad \text{II}$$

$$C^3 = B^2 + a_1 B \qquad \text{III}$$

We can then express a_1, a_3 as

$$a_1 = 3C - 1, \qquad a_3 = -3C^2 - B - 3BC$$

Furthermore, $\text{III} - B\,\text{II}$: $C^3 + 3BC^2 + B^2 \underbrace{(1+a_1)}_{3C} = 0$

$$\rightsquigarrow \quad (C+B)^3 = B^3.$$

Thus for $(E, P_3, Q_3)/S$ with δ affine and $\omega_{E/S}$ free we have defined unique B, C s.t. (E, P_3, Q_3) is the pullback of the universal object as given in the theorem to S, and B, C are independent of a choice of basis of $\omega_{E/S}$.

By gluing, we obtain the same statement for (E, P_3, Q_3) over arbitrary schemes S.

This proves the theorem.