Math 248B. Isogenies and level structures

In this handout, we discussion the notions of isogeny and "level structure" for elliptic curves over schemes.

1. Isogenies

In the analytic theory, we used the local system $\underline{\mathrm{H}}_1(E/M)$ to prove that for a homomorphism $f : E' \to E$ between elliptic curves over a complex manifold, $m \mapsto \deg(f_m)$ is locally constant in M. In particular, if $f_{m_0} = 0$ then $f_m = 0$ for all m near m_0 and if f_{m_0} is a degree-d isogeny then the same holds for f_m when m is near m_0. We need an entirely different method to prove a similar result for elliptic curves over schemes, even when the base is an artin local ring. The main result we are after is this:

Proposition 1.1. *Let $f : E' \to E$ be a homomorphism between elliptic curves over a scheme S. For any integer $d \geq 0$, the locus of $s \in S$ such that $\deg(f_{\overline{s}}) = d$ for a geometric point $\overline{s}$ over s (the choice of which does not matter) is open and closed. If $\deg(f_{\overline{s}}) = d$ for all $\overline{s}$ then f is finite locally free of degree d when $d > 0$ and $f = 0$ when $d = 0$.*

Proof. The reader who likes to avoid noetherian hypotheses is invited to work out the reduction to the noetherian case (hint: we may work Zariski-locally on S, so we can assume S is affine). Thus, we now may and do assume that S is noetherian and then even connected. We will prove that $\deg(f_s)$ is independent of $s \in S$. Every point of S is linked to any other point through finitely many steps of generization or specialization (as the irreducible components must be linked to each other in finitely many steps, and each has a generic point). Any pair of distinct points $\{s, \eta\}$ in a noetherian scheme M with s a specialization of η (i.e., s in the closure of $\{\eta\}$) is hit by a map $\mathrm{Spec}\, R \to M$ with R a discrete valuation ring (with fraction field K). Hence, to prove constancy of the fibral degree we may assume that $S = \mathrm{Spec}\, R$. We may make faithfully flat base change to the completion of a strict henselization, so the finite étale R-group $E'[N]$ is constant for any $N \geq 1$ not divisible by the residue characteristic.

First assume that the map $f_0 : E'_0 \to E_0$ between special fibers vanishes, so the map $E'[N] \to E[N]$ between constant groups vanishes on the special fiber and therefore is 0. In particular, the generic fiber $f_K : E'_K \to E_K$ vanishes on the N-torsion for all N not divisible by $\mathrm{char}(k)$, forcing $f_K = 0$, and hence $f = 0$ (by R-flatness of E' and separatedness of E). Next, assume that f_0 is a degree-d isogeny. The quasi-finite locus U of points $x' \in E'$ that are isolated in their f-fiber is open (by semi-continuity of fiber dimension) and contains E'_0. By R-flatness of E', it follows that U must meet the generic fiber (as it is non-empty) and hence f_K has some points isolated in their fiber. But f_K is a homomorphism, so by homogeneity among its geometric fibers, this map must be isogeny. We conclude that f is quasi-finite, and therefore finite by properness. Moreover, both fibral maps f_K and f_0 are flat, so by the fibral flatness criterion from HW8 we see that f is flat. But being finite flat forces $f : E' \to E$ to have a degree that is locally constant on E, yet E is connected since it is even irreducible (R-flatness of E forces all generic points of E to lie in E_K, yet E_K is irreducible). This proves that f has *constant* fibral degrees, so in particular $\deg(f_0) = \deg(f_K)$ as desired.

Finally, returning to the case of a general (noetherian) base scheme S, we assume $\deg(f_s) = d \geq 0$ for all $s \in S$ and seek to prove that $f = 0$ when $d = 0$ and that f is finite locally free of degree d when $d > 0$. When $d = 0$, the rigidity lemma from class implies that $f = 0$. Now suppose $d > 0$. The fibral flatness criterion from HW8 implies that f is flat, and the properness and quasi-finiteness imply that f is finite. Thus, f is finite locally free (as S is noetherian) and its rank must be d everywhere since every fiber of f is a fiber of some f_s (and we assume that $\deg(f_s) = d$ for all $s \in S$). ∎

Definition 1.2. An *isogeny* $f : E' \to E$ is a homomorphism of S-groups that satisfies $\deg(f_s) \neq 0$ for all $s \in S$. If $\deg(f_s) = d$ for all $s \in S$ then we call f a *degree-d isogeny*.

The preceding proposition shows that isogenies are finite locally free, and that if f is an isogeny then $S = \coprod_{d \geq 1} S_d$ where S_d is the (possibly empty) open and closed subscheme over which f restricts to be finite locally free of degree d.

In order that isogenies be a useful concept, we need to show that they share the familiar "quotient" properties as in the classical theory over an algebraically closed field.

Proposition 1.3. *Let $f : E' \to E$ be an isogeny of elliptic curves. Then the scheme-theoretic kernel $G := \ker f = f^{-1}(e)$ is a finite locally free S-subgroup of E' and $E'/G = E$ in the sense that f is invariant under G-translation on E' and every S-map $h : E' \to X$ that is invariant under G-translation on E' uniquely factors through f. When h is a homomorphism of S-groups, the factorized map $E \to X$ is also an S-homomorphism.*

Proof. Since f is finite locally free as a scheme map, so is the base change $G \to S$ along $e : S \to E$. By definition of G, clearly f is G-invariant. Consider the assertion that every G-invariant S-map $h : E' \to X$ factors uniquely through E. The uniqueness follows from the faithful flatness (i.e., flatness and surjectivity) of f. Likewise, if h is an S-homomorphism and the unique compatible S-map $E \to X$ exists then this latter map is necessarily an S-homomorphism because that property corresponds to an equality of two maps $E \times_S E \rightrightarrows X$, and such an equality can be checked after composing with the faithfully flat map $f \times f : E' \times_S E' \to E \times_S E$.

To construct the desired map $E \to X$, we will use faithfully flat descent theory (explained very elegantly in Chapter 6 of "Néron Models"). The idea is that we view the faithfully flat quasi-compact map $f : E' \to E$ as a "cover" whose "double overlap" corresponds to $E' \times_E E'$. The "agreement on double overlaps" for h corresponds to the condition that composites of h with the two projections $p_1, p_2 : E' \times_E E' \rightrightarrows E'$ coincide. More precisely, fpqc descent theory for scheme morphisms says that the existence of a factorization of h through f is equivalent to the equality of maps $h \circ p_1 = h \circ p_2$. But the definition of G as a scheme-theoretic kernel implies that the natural map of S-schemes $\theta : G \times_E E' \simeq E' \times_E E'$ defined by $(g, y) \mapsto (g + y, y)$ is an isomorphism (thinking functorially). It is therefore harmless to check the desired equality of maps after composing with θ. But $h \circ p_1 \circ \theta : G \times_S E' \to X$ is $(g, y) \mapsto h(g + y)$ whereas $h \circ p_2 \circ \theta$ is given by $(g, y) \mapsto h(y)$. Hence, the fpqc descent criterion is precisely the G-invariance condition on h. ∎

Remark 1.4. In the classical theory, the Frobenius isogeny was used to directly handle problems related to factoring through purely inseparable isogenies. In the relative theory, there is no replacement for the ability to factor an isogeny over a field into an étale part and a tower of Frobenius isogenies. So even over an artin local base, faithfully flat descent is unavoidable.

Now we run the procedure in reserve, constructing an isogeny with any desired kernel. This will be rather more subtle than in the complex-analytic case; without the crutch of exponential uniformizations, we will have to appeal to existence results for quotients in SGA3 (but only in the most concrete situation of affine objects, due to a trick).

Proposition 1.5. *Let $E \to S$ be an elliptic curve, and let $G \subset E$ be a closed S-subgroup such that $G \to S$ is finite locally free. Then an isogeny $q : E \to E'$ exists with kernel G, it is unique up to unique isomorphism (respecting q), and the formation of this quotient $E' = E/G$ commutes with any base change on S.*

The meaning of the compatibility with base change is that the map $E_{S'}/G_{S'} \to (E/G)_{S'}$ induced by $G_{S'}$-invariance of $E_{S'} \to (E/G)_{S'}$ is an isomorphism. Even in the classical setting over an algebraically closed field, some thought is required to construct E/G when G is not étale.

Proof. Base change carries isogenies to isogenies and commutes with the formation of kernels, so Proposition 1.3 takes care of the uniqueness (up to unique isomorphism) and the compatibility with base change. Thus, the only real problem is the construction of E/G. We may work Zariski-locally on S, so we can assume that G has constant order $N \geq 1$. By Deligne's theorem, G is killed by N and hence lies in $E[N]$. This is useful because we have the quotient in our hands for the S-subgroup $E[N]$! Namely $[N] : E \to E$ is an isogeny with kernel $E[N]$. Thus, we are reduced to showing that if $G \subseteq G'$ is an inclusion of finite locally free closed S-subgroups of E and the quotient E/G' exists then the quotient E/G exists. This problem is more tractable because we are looking for E/G as an object intermediate to the finite (hence affine!) map $p : E \to E/G'$.

Since p is G'-invariant, if we view E as a scheme over $T = E/G'$ via p and we introduce the T-group G'_T then we have a natural G'_T-action on E over T. Restricting to a G_T-action, the resulting projections $p_1, p_2 : R := G_T \times_T E \rightrightarrows E$ make R into a "finite locally free equivalence relation" on E over T (i.e.,

the map $(p_1, p_2) : R \to E \times_T E$ is a functorial equivalence relation and p_1 and p_2 are finite locally free). We first seek a quotient by this equivalence relation, which is to say a finite locally free surjective map of T-schemes $E \to E/R$ such that $R = E \times_{E/R} E$ inside of $E \times_T E$; descent theory then forces $E \to E/R$ to be initial among T-maps $h : E \to X$ that are R-invariant in the sense that $E(T') \to X(T')$ is constant on $R(T')$-equivalence classes for all T-schemes T'. (The point of characterizing the quotient E/R as we have is that its formation then clearly commutes with any base change on T.) The existence of such an E/R is a special case of the general problem of existence of a quotient of an *affine* morphism by a finite locally free equivalence relation. The formation of E/R commutes with any base change on S, since that is a special case of base change on T (using $S' \times_S T \to T$ for any $S' \to S$).

By §2(b) in Exposé V of SGA3, such a quotient E/R is provided by Theorem 4.1 in Exposé V of SGA3. Since E/R is built as a kind of "ring of invariants", the construction does not reveal if it has any good structural properties over S. But since $E \to E/R$ is a finite locally free surjection and $E \to T$ is a finite locally free surjection, so is $E/R \to T$ (check!). Thus, $E/R \to S$ is flat and finitely presented (as $T = E/G' \to S$ is so). We claim that E/R is smooth and proper over S with geometric fibers that are curves of genus 1. The properness follows from finiteness over T, and for the other properties we can pass to geometric fibers over S (since the formation of E/R commutes with any base change on S). That is, we may assume $S = \operatorname{Spec} k$ for an algebraically closed field k, and then $E \to E/R$ is a finite flat covering of a proper k-scheme by a smooth connected proper curve. It is then clear that E/R is connected of dimension 1, and since it has a finite *flat* cover by a smooth curve, it must also be a smooth curve (why?). The existence of this cover forces E/R to have genus at most 1, yet E/R covers $T = E/G'$, so its genus cannot be 0.

By composing $E \to E/R$ with the identity section of E, we have equipped E/R with a structure of elliptic curve over S making $E \to E/R$ a homomorphism. This quotient has been designed so that $E \times_{E/R} E = R = G \times_S E$ as subfunctors of $E \times_S E$, so pulling back along the section $e : S \to E$ of the second factor identifies $\ker(E \to E/R)$ with G inside of E. ■

2. Level structures

Now we turn our attention to the structure of torsion in elliptic curves $E \to S$. We largely restrict our attention to $E[N]$ when S is a $\mathbf{Z}[1/N]$-scheme, in which case we know from class that $E[N]_{S'} \simeq (\mathbf{Z}/N\mathbf{Z})^2 \times S'$ as S'-groups for some étale cover $S' \to S$. Recall that a *full level-N structure* on E is an S-group isomorphism $\phi : (\mathbf{Z}/N\mathbf{Z})^2 \times S \simeq E[N]$.

Proposition 2.1. *Let (E, ϕ) be an elliptic curve equipped with a full level-N structure over a $\mathbf{Z}[1/N]$-scheme S. If $N \geq 3$ then (E, ϕ) has no nontrivial automorphism. If $N = 2$ then for an automorphism α of (E, ϕ) there is a clopen decomposition $S = S' \coprod S''$ such that $\alpha = 1$ on $E_{S'}$ and $\alpha = -1$ on $E_{S''}$.*

Proof. We may and do assume that S is noetherian. Then by the rigidity result from class, to prove $\alpha = 1$ when $N \geq 3$ it suffices to do so on geometric fibers. But this case is then classical. Indeed, with $S = \operatorname{Spec} k$ for an algebraically closed field k of characteristic not dividing N, we have $\alpha = 1 + N\beta$ for some $\beta \in \operatorname{End}(E)$, so $\mathbf{Z}[\beta]$ is an order in $\mathbf{Q}$ or a quadratic field such that α is a root of unity (as $\operatorname{Aut}(E)$ is finite). Hence, to settle the case $N \geq 3$ it suffices to show that $1 + N\overline{\mathbf{Z}}$ contains no nontrivial root of unity in $\overline{\mathbf{Q}}$ when $N \geq 3$. Such an N is divisible by 4 or an odd prime, so we can assume $N = p^r \geq 4$ for a prime p. But then the p-adic logarithm and exponential define inverse homomorphisms between $1 + N\overline{\mathbf{Z}}_p$ and $N\overline{\mathbf{Z}}_p$, so $1 + N\overline{\mathbf{Z}}_p$ is multiplicatively torsion-free, as desired.

Now suppose $N = 2$, and return to the case of a general (noetherian) base S. In this case the identity $\alpha = 1 + 2\beta$ implies $\alpha^2 = 1 + 4\beta'$, so α^2 is trivial on $E[4]$. Hence, by the settled case $N = 4$ we have $\alpha^2 = 1$. That is, the commuting endomorphisms $\alpha - 1$ and $\alpha + 1$ having vanishing composition. Their difference [2] is nonzero on all fibers, so they cannot both vanish on any fiber. However, on each fiber they cannot both be isogenies either. It follows that the two subsets $S_\pm = \{s \in S \,|\, \alpha_s = \pm 1\}$ of S are disjoint and cover S. Moreover, by Proposition 1.1 each of S_+ and S_- is open and $\alpha - 1 = 0$ on S_+ and $\alpha + 1 = 0$ on S_-. ■

Theorem 2.2. *Fix $N \geq 1$ and an elliptic curve $E \to S$ over a $\mathbf{Z}[1/N]$ scheme. The contravariant functor on S-schemes defined by*

$$T \rightsquigarrow \operatorname{Isom}_{T\text{-gp}}((\mathbf{Z}/N\mathbf{Z})^2 \times T, E_T[N])$$

is represented by a finite étale cover $I_{E/S,N} \to S$.

Proof. We can reformulate the functor as consisting of ordered pairs (P, Q) in $E[N](T)$ such that the induced map of T-groups

$$(\mathbf{Z}/N\mathbf{Z})^2 \times T = \coprod_{(i,j)\in(\mathbf{Z}/N\mathbf{Z})^2} T \to E_T[N] = E[N]_T$$

(carrying the (i, j)-part to $iP + jQ \in E[N]_T(T) = E[N](T)$) is an isomorphism. To give the ordered pair (P, Q) is to give a map $T \to E[N] \times_S E[N]$, so over $M = E[N] \times_S E[N]$ there is a "universal homomorphism" $h : (\mathbf{Z}/N\mathbf{Z})^2 \times M \to E[N]_M$ of M-groups (given by $(i, j, m) \mapsto ip_1(m) + jp_2(m)$). Hence, we are interested in maps $g : T \to M$ such that $g^*(h) : (\mathbf{Z}/N\mathbf{Z})^2 \times T \to E[N]_T$ is an isomorphism. More specifically, we want to show that this isomorphism condition is equivalent to g factoring through some specific clopen subscheme U of M. One this is done, we can take $I_{E/S,N} = U$; this is finite étale over S since M is finite étale over S, and it is surjective onto S since for any geometric point $\overline{s}$ of S the set $I_{E/S,N}(\overline{s}) = \mathrm{Isom_{gp}}((\mathbf{Z}/N\mathbf{Z})^2, E(\overline{s})[N])$ is clearly non-empty.

Now consider the universal homomorphism $h : (\mathbf{Z}/N\mathbf{Z})^2 \times M \to E[N]_M$. This is a map between finite étale M-schemes of the same rank (N^2), so Zariski-locally on M it is described by a square matrix. The unit condition on the determined corresponds to the isomorphism property, so this is represented by an open subscheme U of M. To prove that U is closed in M, it is equivalent to show that the complement is open. Hence, it suffices to prove that if $h : G \to G'$ is a homomorphism between finite étale group schemes over a scheme M and if it has a nontrivial kernel on some fiber then it has a nontrivial kernel on fibers over all nearby points in M. But the map h is finite étale since G and G' are finite étale over M, so $\ker h$ is finite étale over M. Hence, the order of the geometric fiber of this kernel is Zariski-locally constant on M, and the order is the same as the number of geometric points in the fiber due to the étaleness. ■

Our proof of representability of the full level-3 moduli problem (on the category of schemes over $\mathbf{Z}[1/3]$) will be possible by "bare hands" because the 3-torsion condition has a concrete geometric meaning (related to flex points in the classical case). However, for full level-4 (and beyond) matters are not so accessible by direct arguments. In the remainder of this section, we discuss the additional ideas which are needed to begin the arguments for full level-4.

As a step towards proving representability of the full level-4 moduli problem (on the category of schemes over $\mathbf{Z}[1/4] = \mathbf{Z}[1/2]$), we will introduce the *Legendre moduli problem*, an auxiliary rigid moduli problem that sits between the non-rigid full level-2 and the rigid full level-4 problems. The definition of this problem requires the following notion that relates "Weierstrass coordinates" to relative 1-forms.

Definition 2.3. Let $f : E \to S$ be an elliptic curve over an arbitrary scheme. Assume that the line bundle $\omega_{E/S} = f_*\Omega^1_{E/S}$ is trivial, and let ω be a trivializing section (equivalently, an element of $\mathrm{H}^0(E, \Omega^1_{E/S})$ that restricts to a non-vanishing 1-form on all geometric fibers $E_{\overline{s}}$). If $\{x, y\}$ is a pair of Weierstrass coordinates for $E \to S$ then it is *adapted* to ω if the isomorphisms

$$\omega_{E/S} \simeq \mathscr{I}_e/\mathscr{I}_e^2 \simeq \mathscr{O}(e)/\mathscr{O}_E, \;\; \mathscr{O}(2e)/\mathscr{O}(e) \simeq (\mathscr{O}(e)/\mathscr{O}_E)^{\otimes 2}, \;\; \mathscr{O}(3e)/\mathscr{O}(2e) \simeq (\mathscr{O}(e)/\mathscr{O}_E)^{\otimes 3}$$

carry x mod $\mathscr{O}(e)$ over to $\omega^{\otimes 2}$ and y mod $\mathscr{O}(2e)$ over to $\omega^{\otimes 3}$.

A more concrete version of the definition can be provided when $\mathscr{I}_e$ admits a trivializing section t along $e(S)$ (which always exists Zariski-locally over S, as seen in class): upon unit-scaling t so that $\omega = (1 + t(\dots))\mathrm{d}t$, the condition is that $x = 1/t^2 + (1/t)(\dots)$ and $y = 1/t^3 + (1/t^2)(\dots)$ where "$(\dots)$" denotes a section of $\mathscr{O}_E$ on some open set containing $e(S)$. Thus, if $\{x, y\}$ is adapted to ω, then the same holds for any $\{x+r, y+sx+w\}$, whereas $\{u^2x, u^3y\}$ is adapted to $u^{-1}\omega$ for a unit u on S. In other words, the "adaptation" property removes the ambiguity of unit-scaling in the selection of Weierstrass coordinates (when they exist) via a choice of trivialization section of $\omega_{E/S}$ (when such a section exists!).

Example 2.4. If there exist Weierstrass coordinates $\{x, y\}$ globally over S then we claim that the 1-form

$$\omega = -\frac{\mathrm{d}x}{2y + a_1x + a_3} = -\frac{\mathrm{d}y}{3x^2 + 2a_2x + a_4 - a_1y}$$

which trivializes $\omega_{E/S}$ makes $\{x, y\}$ adapted to ω. Indeed, this problem is local on S, so we can assume there exists a trivializing section t of $\mathscr{I}_e$ on an open set around $e(S)$. We then have $x = v/t^2 + \dots$ and $y = v'/t^3 + \dots$ for units v, v' on S, yet $y^2 - x^3 \in \mathscr{O}(5e)$, so $v'^2 = v^3$. In other words, for $u = v/v'$ we have $u^{-2} = v$ and $u^{-3} = v'$, so $x = 1/(ut)^2 + \dots$ and $y = 1/(ut)^3 + \dots$. Hence, it suffices to show that $\omega = (1 + ut(\dots))\mathrm{d}(ut) = (u + t(\dots))\mathrm{d}t$. By working in stalks over S (as we may), it can be assumed that S is local. Thus, the residue characteristic at the closed point is either not 2 or not 3 (or not both), which is to say that either 2 or 3 is a unit on S. In the former case, we use the first expression for ω to get

$$\omega = \frac{(2/u^2)(1/t^3)(1 + t(\dots))\mathrm{d}t}{(2/(ut)^3)(1 + t(\dots))} = u(1 + t(\dots))\mathrm{d}t,$$

whereas in the latter case we use the second expression for ω to get

$$\omega = \frac{(3/u^3)(1/t^4)(1 + t(\dots))\mathrm{d}t}{(3/(ut)^4)(1 + t(\dots))} = u(1 + t(\dots))\mathrm{d}t.$$

Running this in reverse, suppose a global trivializing section ω of $\omega_{E/S}$ is given and that global Weierstrass coordinates $\{x, y\}$ exist (the latter being automatic when S is affine, as we saw in class). Then we claim that $\{x, y\}$ can *always* be chosen to be adapted to ω. Indeed, make an initial choice of $\{x, y\}$, so the preceding calculation provides a trivializing section η of $\omega_{E/S}$ for which $\{x, y\}$ is adapted to η. But then $\omega = u\eta$ for some global unit u on S, so $\{u^{-2}x, u^{-3}y\}$ is a pair of Weierstrass coordinates adapted to ω.

The definition of a Legendre structure, as an intermediate concept between a full level-2 structure and a full level-4 structure, is best motivated by considering an elliptic curve E over a $\mathbf{Z}[1/2]$-scheme S and a full level-2 structure (P, Q) on E over S. We will use the level-2 structure to partitally "rigidify" a choice of Weierstrass coordinates. Let's first work Zariski-locally on S so that there exist Weierstrass coordinates $\{x, y\}$, and later we will return to the globalization issue. Since 2 is a unit in S we may "complete the square" in y (i.e., replace y with $y + (a_1/2)x + (a_3/2)$) to arrange that the Weierstrass model is

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

In this case the finite étale 2-torsion subscheme can be identified, due to inversion taking on a familiar form:

Lemma 2.5. *Let $y^2 = x^3 + a_2x^2 + a_4x + a_6$ be a smooth Weierstrass cubic over a $\mathbf{Z}[1/2]$-scheme S. Relative to the unique S-group structure with identity $e = [0, 1, 0]$, inversion is given by $[x, y, z] \mapsto [x, -y, z]$.*

Proof. The proposed map is an endomorphism of the pointed curve, so our problem is to prove an equality between two endomorphisms of an elliptic curve. By the rigidity lemma it suffices to check on geometric fibers, where the assertion is classical. ■

In view of the preceding lemma, for such Weierstrass cubics E the degree-4 finite étale S-scheme $E[2]$ meets the affine plane over S in the locus $y = 0$, which is to say the zero-scheme of the cubic $x^3 + a_2x^2 + a_4x + a_6$ in the x-axis. This is finite étale of degree 3 (since it is visibly finite locally free of degree 3, and étale on geometric fibers since the cubic must be separable on geometric fibers), and the identity section splits off (as does any section to a finite étale map, so

$$E[2] = e(S) \coprod (\{x^3 + a_2x^2 + a_4x + a_6 = 0\} \times \{0\}).$$

In more intrinsic terms, we have arranged y so that it vanishes along the non-identity part of $E[2]$. Since we are given a full level-2 structure (P, Q), necessarily $P = (0, a)$, $Q = (0, b)$, $P + Q = (0, c)$ where $(a - b)(a - c)(b - c)$ is a unit on S and the cubic splits as $(x - a)(x - b)(x - c)$. Since we are free to make an additive translation on x, it can be arranged that $x(P) = 0$, which is to say that $bc(b - c)$ is a unit and the cubic has the form $x(x - b)(x - c)$.

A quick inspection of the "transformation formulas" for Weierstrass coordinates shows that to preserve the conditions that y vanishes along $E[2]$ (ie.., the left side of the Weierstrass equation is y^2) and $x(P) = 0$, we may only make the changes $(x', y') = (u^2x, u^3y)$ for a unit u. This leads to the new equation $y'^2 = x'(x' - bu^2)(x' - cu^2)$. Thus, $x(Q) = b$ is a unit on S which only changes by unit squares as we vary through the possible Weierstrass cubics. On the other hand, we can keep track of the unit u exactly by using the

trivialization ω of $\omega_{E/S}$ with respect to which the Weierstrass coordinates are adapted (Example 2.4). This essentially proves:

Lemma 2.6. *Let $(E,(P,Q))$ be an elliptic curve equipped with a full level-2 structure over a $\mathbf{Z}[1/2]$-scheme S. If there exists a trivializing section ω of $\omega_{E/S}$ then there exists a unique pair $\{x,y\}$ of global Weierstrass coordinates on E adapted to ω such that $y|_{E[2]}=0$ and $x(P)=0$. Moreover, as we vary through all choices of ω, the corresponding adapted coordinates $\{x,y\}$ satisfy the condition that the value $x(Q)$ sweeps out an entire class in $\mathscr{O}(S)^\times/(\mathscr{O}(S)^\times)^2$.*

Proof. The preceding argument proves the lemma *if* there exists some global Weierstrass coordinates. But in view of the uniqueness part of the assertion, to prove the lemma in general we may work Zariski-locally on the base! Hence, we can reduce to the case when such global coordinates do exist, and then apply the preceding considerations. ■

Now consider $(E,(P,Q))$ as above, and suppose there exists a trivializing section ω of $\omega_{E/S}$. In terms of the associated Weierstrass coordinates $\{x,y\}$ as in the lemma, the condition that $x(Q)$ is a *square* is independent of the choice of ω. This is then an intrinsic property of $(E,(P,Q))$, and when it holds we may choose a square root so as to obtain an ω_0 for which the associated coordinates $\{x_0,y_0\}$ satisfy $x_0(Q)=1$. Note that ω_0 is unique up to μ_2-scaling, and in such coordinates E takes the form

$$y_0^2=x_0(x_0-1)(x_0-\lambda)$$

where $\lambda(1-\lambda)$ is a unit on S and $P=(0,0)$ and $Q=(0,1)$.

Now we are ready to introduce a new level structure.

Definition 2.7. Let E be an elliptic curve over a $\mathbf{Z}[1/2]$-scheme. A *Legendre structure* on E is a pair $(\omega,\phi=(P,Q))$ consisting of a trivializing section ω of $\omega_{E/S}$ and a full level-2 structure (P,Q) of E such that the unique adapted coordinates $\{x,y\}$ satisfying $y|_{E[2]}=0$ and $x(P)=0$ also satisfy $x(Q)=1$.

Remark 2.8. Although we can always modify a Legendre structure via μ_2-scaling of ω (which has no effect on x and induces the same μ_2-scaling on y), beware that $\mathrm{GL}_2(\mathbf{Z}/2\mathbf{Z})$ *does not act on Legendre structures.* That is, if we modify the choice of full level-2 structure via the action of a nontrivial element of $\mathrm{GL}_2(\mathbf{Z}/2\mathbf{Z})=S_3$ then typically the new full level-2 structure does *not* admit an associated Legendre structure. Indeed, the condition $y|_{E[2]}=0$ is insensitive to the specific choice of full level-2 structure, whereas the condition $x(P)=0$ serves solely to eliminate the additive translation on x, so an intrinsic formulation of the existence of a Legendre structure associated to a given $(E,\omega,(P,Q))$ is the property that $x(Q)-x(P)$ is a square in S. (Note that global Weierstrass coordinates may not exist when S is not affine, but Zariski-locally they exist and when we then choose them adapted to ω so that $y|_{E[2]}=0$, the difference $x(Q)-x(P)$ is a unit that is insenstive to the remaining ambiguity of additive translation in x and hence it is intrinsic and globalizes to an element of $\mathscr{O}(S)^\times$. Is is the square property for this global unit that characterizes the existence or not of a Legendre structure compatible with the given data $(E,\omega,(P,Q))$.)

To make the preceding remark more explicit, consider the elliptic curve $y^2=x(x-1)(x-\lambda)$ over a scheme S (so $\lambda(1-\lambda)$ is a unit, encoding the smoothness). The key issue is that typically the five differences

$$x(\phi\circ g(0,1))-x(\phi\circ g(1,0))=\{-1,\pm\lambda,\pm(1-\lambda)\}$$

for nontrivial $g\in\mathrm{GL}_2(\mathbf{Z}/2\mathbf{Z})$ are all non-squares on S. However, in the Katz–Mazur book, this problem (i.e., the need to select a square root of $x(Q)$) was overlooked and it was mistakenly claimed in (4.6.2) that the functor of Legendre structures has a natural action by $\mathrm{GL}_2(\mathbf{Z}/2\mathbf{Z})\times\langle-1\rangle$ (creating a torsor for that finite group). This non-existent action was "used" at the bottom of all moduli scheme constructions where the crutch of full level-3 is not available (i.e., near points of residue characteristic 3). Thus, the construction technique in Katz–Mazur needs to be corrected. The simplest way out seems to be to make a direct attack on the full level-4 moduli problem (which does admit a useful finite group action, namely by $\mathrm{GL}_2(\mathbf{Z}/4\mathbf{Z})$). This is done below, with the Legendre problem nonethless serving as a useful intermediate step.

3. Existence of $Y(4)$ over $\mathbf{Z}[1/4] = \mathbf{Z}[1/2]$

In this section we construct $Y(4)$. The case of $Y(3)$ is somewhat simpler, so the reader may prefer to read that case first; see §4. As a first step towards building $Y(4)$, we prove the rigidity of Legendre structures and compute an explicit universal object for the Legendre moduli problem (thereby proving representability of this moduli problem) on the category of $\mathbf{Z}[1/2]$-schemes.

Proposition 3.1. *Legendre structures are rigid, and the contravariant functor assigning to any $\mathbf{Z}[1/2]$-scheme S the set of isomorphism classes of tuples $(E, \omega, (P, Q))$ consisting of an elliptic curves over S equipped with a Legendre structure is representable. A universal structure is given by the elliptic curve $y^2 = x(x-1)(x-\lambda)$ over $\mathbf{Z}[1/2][\lambda][1/\lambda(1-\lambda)]$, equipped with $\omega = -\mathrm{d}x/2y$ and the full level-2 structure $P = (0,0)$ and $Q = (0,1)$.*

Proof. To prove the rigidity we may work Zarski-locally on S, so by the case $N = 2$ in Proposition 2.1 it suffices to rule out inversion on E. Since inversion has the effect of scaling by -1 on the relative tangent space (as for any smooth group scheme, due to the fact that the group law always induces addition on the relative tangent space), and hence on $\omega_{E/S} \simeq e^*(\Omega^1_{E/S}) = \mathrm{Tan}_e(E)^\vee$, the condition of respecting the trivializing section ω of $\omega_{E/S}$ eliminates inversion from consideration. Hence, rigidity holds.

The argument preceding Definition 2.7 and the parenthetical observations on globalization in Remark 2.8 show that any $(E, \omega, (P, Q))$ over any S admits a global Weierstrass model that is a pullback of the proposed universal structure along some morphism $\lambda : S \to \mathbf{G}_m - \{1\}$. By rigidity, the isomorphism of E to such a Weierstrass model (respecting the Legendre structures) is *unique*. We have seen that there exist *unique* global Weierstrass coordinates $\{x, y\}$ for E adapted to ω such that $y|_{E[2]} = 0$, $x(P) = 0$, and $x(Q) = 1$, so this proves the uniqueness of $\lambda : S \to \mathbf{G}_m - \{1\}$. ∎

One further ingredient is needed before we can build a universal elliptic curve equipped with a full level-4 structure. We need to show that full level-4 structures always "dominate" Legendre structures in a canonical manner.

Proposition 3.2. *Let E be an elliptic curve over a $\mathbf{Z}[1/2]$-scheme S, and let $P \in E[2](S)$ and $Q_4 \in E[4](S)$ be such that $(P, [2](Q_4))$ is a full level-2 structure. There is a canonically associated Legendre structure $(E, \omega, (P, [2](Q_4)))$, and negating Q_4 has the effect of negating ω.*

Implicit in the canonicity is the compatibility with base change.

Proof. Since we will make a construction that is canonical, it suffices to work Zariski-locally. Hence, we can assume there exist Weierstrass coordinates $\{x, y\}$ of E, and they may then (as above) be chosen to satisfy $y|_{E[2]} = 0$ and $x(P) = 0$. We may write the elliptic curve in the non-Weierstrass form

$$y^2 = ux(x-1)(x-\lambda)$$

where $\lambda(1-\lambda)$ is a unit and u is a unit. Writing $Q_4 = (a, b)$, we must have that b is a unit (since $[2](Q_4)$ has exact order 2 on geometric fibers, so b is nonzero on geometric fibers), and also a is a unit (since a divides b^2 due to the Weierstrass equation). Likewise, $a - 1$ is a unit.

We claim that the condition $[2](Q_4) = (0, 1)$ implies that

$$u = \left(\frac{-u(3a^2 - 2a(\lambda+1) + \lambda)}{2b} + \frac{b}{a}\right)^2.$$

To prove this we may assume that $S = \mathrm{Spec}\, R$ for an R that is local, then noetherian, and then (by faithful flatness) complete. As such, R is the quotient of a complete regular local ring R', and we can lift E to an elliptic curve E' over R' by lifting u and λ to $u', \lambda' \in R'$ respectively. The R'-scheme $E'[4]$ is finite étale, so by the completion of R' the section $Q_4 \in E'[4](R) = E[4](R)$ satisfying $[2](Q_4) = (0, 1)$ must uniquely lift to a section Q_4' of $E'[4]$ over R' with the same properties. Writing $Q_4' = (a', b')$, necessarily a' lifts a and b' lifts b. Hence, it suffices to prove the desired identity over R', so we have finally reduced to the case when the base is regular local and therefore a *domain*. This injects into an algebraically closed field, so we have finally reduced to a classical situation. In this setting, the equation $[2](a, b) = (1, 0)$ says exactly that the tangent

line through (a,b) passes through the point $(1,0)$ (which is distinct from (a,b), since $b \neq 0$). By computing the equation for the tangent line at (a,b) and evaluating it at $(1,0)$, the vanishing of such evaluation gives exactly the desired identity.

To summarize, the specification of Q_4 provides a canonical choice of square root of u, so dividing y by that square root yields (with $\omega = -\mathrm{d}x/2y$) a Legendre structure $(E, \omega, (P, [2](Q_4)))$. It is clear that this construction is canonical, and if we negative Q_4 then b is negated and hence the specified square root of u is negated. The resulting effect on $\{x, y\}$ is to negate y, so $\omega = -\mathrm{d}x/2y$ is also negated. ■

Theorem 3.3. *The functor assigning to any $\mathbf{Z}[1/2]$-scheme S the set of isomorphism classes of pairs (E, ϕ_4) consisting of an elliptic curve E over S equipped with a full level-4 structure ϕ_4 is represented by an affine $\mathbf{Z}[1/2]$-scheme $Y(4)$ of finite type.*

Proof. Recall from class that full level-4 structure are rigid. By Proposition 3.2, we can describe any pair (E, ϕ_4) up to *unique* isomorphism as follows. We form a Legendre structure $(E, \omega, (P_2, Q_2))$ over S, along with a specified 4-torsion point $Q_4 \in E[4](S)$ such that $[2](Q_4) = Q_2$. Then we simply specify $P_4 \in E[4](S)$ such that $[2](P_4) = P_2$. The reason that this works is that to check if a map of S-groups $(\mathbf{Z}/4\mathbf{Z})^2 \times S \to E[4]$ is an isomorphism, it is equivalent to check that the induced map $(\mathbf{Z}/2\mathbf{Z})^2 \times S \to E[2]$ between 2-torsion subgroups is an isomorphism. Indeed, due to both sides being finite étale, the isomorphism property over S is equivalent to the same on geometric fibers over S, where we can apply the elementary fact that a homomorphism between two finite free $\mathbf{Z}/(p^2)$-modules of the same rank is an isomorphism if and only if it is so on the p-torsion subgroups.

Now the whole process can be done in reverse. By Proposition 3.1, the Legendre moduli problem is represented by an affine $\mathbf{Z}[1/2]$-scheme of finite type (even open in the affine line over $\mathbf{Z}[1/2]$). Let $(E \to M, \omega, (P, Q))$ be a universal such structure. Now consider the finite étale cover $M' = [2]^{-1}(Q) \to M$. Over M' we have the universal structure $(E' = E_{M'}, (P_{M'}, Q'))$ making $(P_{M'}, [2](Q') = Q_{M'})$ a full level-2 structure. But there is also the trivialization section $\omega_{M'}$ of $\omega_{E'/M'}$, and Proposition 3.2 enhances $(E', (P_{M'}, [2](Q')))$ to a Legendre structure $(E', \omega', (P_{M'}, [2](Q')))$. Does $\omega_{M'} = \omega'$? Well, we already know that $(E, \omega, (P, Q))$ is a Legendre structure, so by base change $(E', \omega_{M'}, (P_{M'}, Q_{M'} = [2](Q')))$ is also a Legendre structure. Hence, $\omega' = \varepsilon\omega_{M'}$ where $\varepsilon \in \mu_2(M')$. Since M' is a $\mathbf{Z}[1/2]$-scheme, the conditions $\varepsilon = \pm 1$ define a partition of M' into disjoint open subschemes $M'_{\pm}$. By construction, the open subscheme M'_+ is the *universal* triple $(\mathscr{E} \to \mathscr{M}, \mathscr{P}_2, \mathscr{Q}_4)$ consisting of an elliptic curve over a $\mathbf{Z}[1/2]$-scheme equipped with a 2-torsion section $\mathscr{P}_2$ and 4-torsion section $\mathscr{Q}_4$ such that $(\mathscr{P}_2, [2](\mathscr{Q}_4))$ is a full level-2 structure. (Make sure you understand why this is really universal as such, including that there are no rigidity problems.)

Finally, consider the finite étale cover $M'' = [2]^{-1}(P_{M'_+}) \to M'_+$. By the universal property of the restriction of $(E', P_{M'}, Q')$ over M'_+, it follows that M'' represents the moduli problem of triples consisting of an elliptic curve over a $\mathbf{Z}[1/2]$-scheme and a pair of 4-torsion sections whose doubles are a full level-2 structure. But that is exactly the same thing as an elliptic curve equipped with a full level-4 structure! Hence, M'' is the desired moduli scheme. ■

Remark 3.4. By construction, $Y(4)$ is finite étale over $\mathbf{Z}[1/2][\lambda][1/\lambda(1-\lambda)]$ (and surjective, since over an algebraically closed field not of characteristic 2 any Legendre structure can be "promoted" to a full level-4 structure, reversing Proposition 3.2. Hence, $Y(4)$ is regular and $Y(4) \to \mathbf{Z}[1/2]$ is smooth and affine with all fibers of pure dimension 1. What is rather less evident is whether $Y(4)$ is connected, or how to describe the connected components of its geometric fibers in various characteristics. This will be answered (even for characteristic > 2!) by using compactificactions of modular curves, comparison with the complex-analytic theory, and Stein factorization. Such a method is all that is known for other moduli spaces too, such as for curves, abelian varieties, etc.

4. Existence of $Y(3)$ over $\mathbf{Z}[1/3]$

This section is aimed at proving the representability of the full level-3 moduli problem on the category of $\mathbf{Z}[1/3]$-schemes. The result is much easier to write out explicitly than for full level-4, and the proof as well is rather simpler (e.g., there are no complications caused by needing to "adapt" Weierstrass coordinates

to a particular trivialization of $\omega_{E/S}$). We first state the main result, and then build up towards the proof in several stages. Loosely speaking, the idea will be to use the level structure to single out a preferred Weierstrass model characterized by intrinsic properties (related to the level structure). This uniqueness will permit globalization, and the presence of the full level-3 structure will impose algebraic relations on the coefficients of the Weierstrass cubic. Those relations in turn will define $Y(3)$ as an affine scheme of finite type over $\mathbf{Z}[1/3]$. Our arguments below are just a more detailed version of calculations in Katz–Mazur.

Theorem 4.1. *The moduli functor of full level-3 structure on the category of $\mathbf{Z}[1/3]$-schemes is represented by a smooth affine $\mathbf{Z}[1/3]$-scheme $Y(3)$ of pure relative dimension 1. Explicitly,*

$$Y(3) = \operatorname{Spec} \mathbf{Z}[1/3][B,C][((a_1^3 - 27a_3)a_3C)^{-1}]/(B^3 - (C+B)^3)$$

with $a_1 = 3C - 1$, $a_3 = -3C^2 - B - 3BC$, and the universal structure

$$E : (y^2 + a_1xy + a_3y = x^3), \quad P = (0,0), \quad Q = (C, B+C).$$

Remark 4.2. This Weierstrass cubic model for the universal elliptic curve E over $Y(3)$ has discriminant $\Delta = a_3^3(a_1^3 - 27a_3)$ and $c_4 = a_1(a_1^2 - 24a_3)$, so $j_{E/Y(3)} : Y(3) \to \mathbf{A}^1_{\mathbf{Z}[1/3]}$ is given by the global function c_4^3/Δ (which is quite nasty and unilluminating if fully written out in terms of B and C). The shape of the Weierstrass cubic corresponds to $(0,0)$ being a 3-torsion section, and the localizations in the description of $Y(3)$ precisely ensure that Δ is a unit and Q is everywhere disjoint from $\pm P$. The relation on B and C corresponds to Q being a 3-torsion section. These features will all emerge from the proof of the theorem.

It will be convenient to compute inversion on some sections, so we begin by recording the formula for inversion on a general smooth Weierstrass cubic; this formula is identical to the familiar one from the classical case.

Lemma 4.3. *Let $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ be a smooth Weierstrass cubic in $\mathbf{P}^2_S$ over an arbitrary scheme S. The inversion endomorphism is given by*

$$(x,y) \mapsto (x, -y - a_1x - a_3),$$

or more precisely $[x,y,z] \mapsto [x, -y - a_1x - a_3z, z]$.

Proof. The appearances of y in the cubic relation all occur on the left side, which factors as $y(y + a_1x + a_3)$. It is thereby clear that the proposed map (which is visibly an automorphism of $\mathbf{P}^2_S$) is an endomorphism of the elliptic curve preserving e. Hence, to check its agreement with inversion we may use the rigidity lemma to reduce to checking on geometric fibers. But this is exactly the classical setting where the formula for inversion is well-known. ∎

Consider a general elliptic curve $E \to S$ over a $\mathbf{Z}[1/3]$-scheme and a full level-3 structure (P,Q) on E. We will use P and Q as crutches to single out a particularly nice Weierstrass form for E that is constructed Zariski-locally on S but always uniquely determined, and hence it will globalize. So at the outset we don't worry about globalization and we work Zariski-locally on S. More specifically, we assume $S = \operatorname{Spec} R$ is affine and that $\omega_{E/S}$ is trivial, so there exists some Weierstrass coordinates $\{x,y\}$ on E over R. Let's first focus on the condition that P is a 3-torsion section which moreover has exact order 3 on geometric fibers (or equivalently, has associated map between finite étale S-groups $(\mathbf{Z}/3\mathbf{Z}) \times S \to E[3]$ that is a closed immersion). Having exact order 3 on geometric fibers (in the presence of the 3-torsion property) amounts to P being disjoint from e as sections, or in other words that P is supported entirely in the affine plane; i.e., $P = (a,b)$ for some $a, b \in R$. The 3-torsion property says, after some Zariski-localization on S (to remove the effect of δ_e as in the definition of the S-isomorphism $E \simeq \mathrm{Pic}^0_{E/S,e}$ that defines the unique S-group law on (E,e)), exactly that $\mathscr{I}_P^3 \simeq \mathscr{I}_e^3$ as $\mathscr{O}_E$-modules. We want to express this property in more hands-on terms.

Loosely speaking, the entire point of the argument that follows is to rigorously justify certain arguments over a ring that are classically carried over over an algebraically closed field (where we can appeal to notions from classical algebraic geometry, such as "tangent line" and "mth-order zero", that are rather more subtle when the base is not a field). We will being by assume P is 3-torsion with exact order 3 on geometric fibers,

deduce an explicit description of (E, P) with $P = (0, 0)$, and then show that the explicit description implies conversely that the point $(0, 0)$ is 3-torsion with exact order 3 on the geometric fibers.

Since P is disjoint from e, the ideal sheaf $\mathscr{I}_P^3$ coincides with O_E near e. Hence, there is a natural inclusion $\mathscr{O}_E \simeq \mathscr{I}_P^3 \otimes_{\mathscr{O}_E} \mathscr{I}_e^{-3} \hookrightarrow \mathscr{I}_e^{-3} = \mathscr{O}(3e)$, and we consider the associated "leading coefficient" map

$$f_*(\mathscr{I}_P^3 \otimes \mathscr{I}_e^{-3}) \hookrightarrow f_*(\mathscr{O}(3e)) \twoheadrightarrow \mathscr{O}_S \tag{4.1}$$

whose formation commutes with any base change on S (why?). This composite map is an *isomorphism*. Indeed, we may pass to geometric fibers, and then this map becomes the natural map carrying an element of the line $\mathrm{H}^0(E_{\overline{s}}, 3e(\overline{e}) - 3P(\overline{s}))$ to its 3rd-order polar coefficient at the origin (according to a local parameter there that is adapted to the initial choice of trivialization of $\omega_{E_{\overline{s}}}$ made at the outset). We simply want this map not to vanish, which is to say that the nonzero rational functions on $E_{\overline{s}}$ with at most a 3rd-order pole at $e(\overline{s})$, at least a 3rd-order zero at $P(\overline{s})$, and no other poles actually do have a 3rd-order pole at the origin (and not at most 2nd-order). But this is clear, since the presence of a 3rd-order zero at the nontrivial $P(\overline{s})$ and the avoidance of poles away from the origin forces the pole at the origin to be of order at least 3 when the rational function is nonzero. (In classical terms, the fact that such a nonzero rational function exists is precisely the "flex-point" condition on nonzero 3-torsion points away from characteristic 3.)

Since $\mathrm{lead}_3(y) = 1$, we conclude from the isomorphism (4.1) that there is a unique generating section of $\mathscr{I}_P^3\mathscr{I}_e^{-3}$ having the form $y + sx + t$. Renaming this as y (as we may do!) then brings us to the case where y is a generating section of $\mathscr{I}_P^3\mathscr{I}_e^{-3}$. In particular, since P is disjoint from e, y is a local generator of $\mathscr{I}_P^3$ near P; loosely speaking, y has a "triple zero" along P. (If the base scheme were a field, this would be literally true. Over a more general base, the concept of "order of a zero" is not reasonable in complete generality, due to the possibility of leading polar coefficients that are nonzero yet also not units.) In particular, $y(P) = 0$. We also replace x with $x - x(P)$ to arrange that $x(P) = 0$. That is, we now have the Weierstrass cubic form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x, \;\; P = (0, 0).$$

By Lemma 4.3 we have $-P = (0, -a_3)$, so the condition of $-P$ being everywhere disjoint from P (a consequence of P being 3-torsion) says that a_3 is a unit. But in view of this disjointness, $\mathscr{I}_P\mathscr{I}_{-P}\mathscr{I}_e^{-2}$ coincides with $\mathscr{I}_P$ near P and $\mathscr{I}_{-P}$ near $-P$, and globally it is naturally a subsheaf of $\mathscr{I}_e^{-2}$. As such, x is a section of this subsheaf (due to $x(P) = 0$ and $x(-P) = 0$), and it generates this sheaf on all geometric fibers! Indeed, on geometric fibers we have the classical situation that x is a rational function with a double pole at the origin, no other poles, and zeros at each of two distinct points. Hence, those zeros must be simple and moreover be the only zeros, whence x generates the predicted line bundle on the geometric fibers. To summarize:

Lemma 4.4. *When x is additively translated so that $x(P) = 0$, then x is a global generator of $\mathscr{I}_P\mathscr{I}_{-P}\mathscr{I}_e^{-2}$. In particular, x has a simple zero along P in the sense that it generates the line bundle $\mathscr{I}_P$ near P.*

Now look at the cubic relation $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x$ near P! The left side is a section of $\mathscr{I}_P^3$ near P, as is x^3, so $a_2x^2 + a_4x$ is as well. But x generates $\mathscr{I}_P$ near P, so under the identification of $\mathscr{O}_E/\mathscr{I}_P^3$ with $R[x]/(x^3)$ (!) we have that $a_2x^2 + a_4x$ vanishes in $R[x]/(x^3)$. This forces $a_2 = a_4 = 0$, so we finally arrive at a much-simplified Weierstrass model:

Lemma 4.5. *In suitable Weierstrass coordinates $\{x, y\}$ such that y generates $\mathscr{I}_P^3$ near P and $x(P) = 0$, the cubic model has the form*

$$y^2 + a_1xy + a_3y = x^3, \;\; P = (0, 0), \;\; (a_1^3 - 27a_3)a_3^3 = \Delta \in \mathscr{O}(S)^\times.$$

Now we run the process in reverse: consider a Weierstrass cubic E as in Lemma 4.5 (necessarily smooth, due to the unit condition). We claim that the shape of the cubic forces $P = (0, 0)$ to be 3-torsion and exact order 3 on all geometric fibers, with y generating $\mathscr{I}_P^3\mathscr{I}_e^{-3}$ and x generating $\mathscr{I}_P\mathscr{I}_{-P}\mathscr{I}_e^{-2}$. Moreover, we claim that under these conditions, the only permissible changes of Weierstrass coordinates that preserve the basic form in Lemma 4.5 are $(x, y) \mapsto (u^2x, u^3y)$ for a unit u on S (which clearly do preserve the given form).

The given cubic model implies $-P = (0, -a_3)$ with a_3 a unit, so P is disjoint from $-P$ and hence x is a section of $\mathscr{I}_P\mathscr{I}_{-P}\mathscr{I}_e^{-2}$. In fact, x generates this line bundle, as it suffices to check this on geometric fibers,

where we can appeal to the classical fact that a rational function on an elliptic curve with a double pole at one point, no other poles, and zeros at two other distinct points must have simple zeros there and nothing else in its divisor (due to the pole being only of order 2). Hence, x generates $\mathscr{I}_P$ near P. But since x and y vanish at P yet a_3 is a unit, it follows that $y+a_1x+a_3$ is a unit on E near P. The left side of the Weierstrass relation factors as $y(y+a_1x+a_3)$, so since x^3 generates $\mathscr{I}_P^3$ near P we conclude from the Weierstrass cubic form that y also generates $\mathscr{I}_P^3$ near P. But y is a section of $\mathscr{I}_e^{-3}$ and P is disjoint from e, so we conclude that y is a section of $\mathscr{I}_P^3\mathscr{I}_e^{-3}$ that is a generator along P and e. This actually forces y to be a global generator of the line bundle. Indeed, we may pass to geometric fibers and then invoke the classical fact that a rational function on an elliptic curve with a triple pole at one point, no other poles, and at least a triple zero at another point must have exactly a triple zero there and nothing else in its divisor. The property that y generates $\mathscr{I}_P^3\mathscr{I}_e^{-3}$ implies that this line bundle is trivial on E, and hence (by the very construction of the group law on E via $\mathrm{Pic}^0_{E/S,e}$) that $[3]P = e$ in the group law on $E(S)$. Thus, we have indeed reversed the entire preceding process. Moreover, the only Weierstrass coordinate changes that preserve the special form (including that $P = (0,0)$) are exactly $(x,y) \mapsto (u^2x, u^3y)$ for a unit u. Indeed, the vanishing of $x(P)$ permits no additive translation on x, and the fact that x generates $\mathscr{I}_P$ near P whereas y generates $\mathscr{I}_P^3$ near P implies that any $u^3y + sx + t$ has image in $\mathscr{O}_E/\mathscr{I}_P^3 = R[x]/(x^3)$ represented by $sx + t$. This can only vanish when $s = t = 0$. Let's summarize our conclusions thus far:

Lemma 4.6. *If (E,P) is an elliptic curve over a $\mathbf{Z}[1/3]$-scheme and P is a section of $E[3]$ with exact order 3 on all geometric fibers then Zariski-locally on the base it admits the form as in Lemma 4.5, and the Weierstrass coordinates are uniquely determined up to $(x,y) \mapsto (u^2x, u^3y)$ for a unit u. Moreover, conversely all instances of the explicit form in Lemma 4.5 satisfy the properties that P is a 3-torsion section with exact order 3 on all geometric fibers, and automatically y generates $\mathscr{I}_P^3\mathscr{I}_e^{-3}$ and x generates $\mathscr{I}_P\mathscr{I}_{-P}\mathscr{I}_e^{-2}$.*

Now let's impose the extra data of a 3-torsion section Q that is fiberwise disjoint from e (equivalently, exact order 3 on fibers) as well as disjoint from $\pm P$ (equivalently, (P,Q) is a full level-3 structure!). As with the above analysis, first we assume some such Q is given and we will use it to *uniquely* specify the Weierstrass coordinates (i.e., eliminate the remaining unit-scaling ambiguity), and we will show that the conditions on Q then impose some explicit relations on the coefficients a_1 and a_3. Then we will reverse the process by proving that those relations on a_1 and a_3 conversely imply that Q (expressed in a special form) is necessarily part of a full level-3 structure together with P. We will have then constructed a universal object for the rigid full level-3 moduli problem on the category of $\mathbf{Z}[1/3]$-schemes.

Taking the full level-3 structure (P,Q) as given, with (E,P) given by the special form as in Lemma 4.5, the same exact arguments as used earlier for P imply that after some Zariski-localization on $S = \mathrm{Spec}\, R$ the line bundle $\mathscr{I}_Q^3\mathscr{I}_e^{-3}$ has a unique generator of the form $y - Ax - B$, and that $x - x(Q)$ generates $\mathscr{I}_Q$ near Q.

Lemma 4.7. *The element $A \in R$ is a unit.*

Proof. Everything commutes with base change, so by passing to geometric points over S we may assume that R is an algebraically closed field. We assume $A = 0$ and seek a contradiction. By hypothesis, $A = 0$ implies that $y - B$ has a triple zero at Q, so $x(Q)$ is a triple zero of the polynomial in x obtained by substituting $y = B$ into the special Weierstrass form. In other words, $x^3 - Ba_1x + (a_3B + B^3)$ has a triple zero at $x(Q)$. But we're not in characteristic 3 (!), so the vanishing of the x^2-term in this polynomial implies that the triple zero $x(Q)$ must vanish. But the special Weierstrass form meets $x = 0$ in the affine plane in the locus $y^2 + a_3y = 0$ in the y-axis. This is precisely $(0,0) = P$ and $(0,-a_3) = -P$, contradicting that (P,Q) is a full level-3 structure. ∎

Thanks to this lemma, by taking $u = A$ the change of variable $(x,y) \mapsto (u^2x, u^3y)$ carries $y - Ax - B$ to $u^3(y - x - B/u^3)$, so in these new coordinates some unique $y - x - B$ generates $\mathscr{I}_Q^3\mathscr{I}_e^{-3}$. In view of how we arrived at this situation, we see that this latter condition (together with the earlier conditions on the special Weierstrass form) *uniquely determines* the Weierstrass coordinates.

Letting $C = x(Q)$, since $y - x - B$ vanishes at Q (in fact, lies in $\mathscr{I}_Q^3$ near Q) we have $Q = (C, C + B)$. The condition that $y - x - B$ generates $\mathscr{I}_Q^3$ near Q implies that when the relation $y = x + B$ is substituted into

the special Weierstrass form the resulting polynomial in x vanishes in $\mathscr{O}_E/\mathscr{I}_Q^3 = R[x]/(x-C)^3$. In other words, the cubic polynomial

$$x^3 - ((x+B)^2 - (a_1x + a_3)(x+B))$$

vanishes in $R[x]/(x-C)^3$, which is to say (by consideration of x^3-terms) that

$$x^3 - ((x+B)^2 - (a_1x + a_3)(x+B)) = (x-C)^3$$

in $R[x]$. Comparing coefficients in x-degrees 0, 1, and 2, we arrive at precisely the relations

$$3C = a_1 + 1, \;\; 3C^2 = 2B + a_1B + a_3, \;\; C^3 = B^2 + a_3B.$$

These can be rewritten in the following more convenient form:

$$a_1 = 3C - 1, \;\; a_3 = -3C^2 - B - 3BC, \;\; B^3 = (C+B)^3.$$

Here, $P = (0,0)$ and $Q = (C, C+B)$ with C a *unit*: this unit condition exactly says that on geometric fibers Q avoids the locus in the affine plane where E meets $\{x = 0\}$, which is exactly $\{P, -P\}$. In other words, C being a unit encodes precisely that (P,Q) is a full level-3 structure (given that P and Q are 3-torsion sections).

Now we run the procedure in reverse:

Lemma 4.8. *In the ring* $\mathbf{Z}[1/3][B,C]$*, define* $a_1 = 3C - 1$ *and* $a_3 = -3C^2 - B - 3BC$*. Define* $\Delta = a_3^3(a_1^3 - 27a_3)$*, and let* E *be the Weierstrass cubic*

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

over $\mathbf{Z}[1/3][B,C][1/(\Delta C)]/((B^3 - (B+C)^3)$*. The points* $P = (0,0)$ *and* $Q = (C, B+C)$ *form a full level-3 structure on* E*, and these Weierstrass coordinates are the unique ones for* E *which satisfy the indicated special form and make the section* $y - x - B$ *of* $\mathscr{I}_Q$ *lie in* $\mathscr{I}_Q^3$*.*

Before proving the lemma, we make some observations. The key point is that since such Weierstrass coordinates have been *uniquely* characterized, the process leading up to their construction Zariski-locally on the base for any elliptic curve equipped with full level-3 structure over a $\mathbf{Z}[1/3]$-scheme can then be carried out *globally* (i.e., the constructions locally on the base must coincide on overlaps and hence glue). Thus, the above explicit form is a universal object for the full level-3 moduli problem, and so the proof of Theorem 4.1 will be completed. (The fact that the coordinate ring of this moduli scheme is smooth of pure relative dimension 1 over $\mathbf{Z}[1/3]$ is clear by inspection, as follows. If we ignore the localization at Δ we have the algebra $\mathbf{Z}[1/3][B,C][1/C]/(B^3 - (C+B)^3)$, whose geometric fibers over $\operatorname{Spec}\mathbf{Z}[1/3]$ have the form $k[u,v,1/(u-v)]/(u^3 - v^3)$. This is a smooth curve because the singularities on $u^3 = v^3$ occur at the origin, where $u - v$ is not invertible. See §5 for the "right" proofs of smoothness and pure relative 1-dimensionality via functorial methods, as is required for the general study of moduli spaces.)

Proof. Since C is a unit in the base ring, Q is disjoint from $\pm P$ (as well as from e). The definitions of a_1 and a_3 in terms of B and C, together with the relation $B^3 = (C+B)^3$, have been seen to encode exactly the condition that the global section $y - x - B$ of $\mathscr{I}_e^{-3}$ also lies in $\mathscr{I}_Q^3$ near Q, and hence is a global section of $\mathscr{I}_Q^3\mathscr{I}_e^{-3}$. We claim that necessarily $y - x - B$ generates this line bundle. To verify this claim it suffices to check on geometric fibers, where we may appeal to the classical fact that a rational function on an elliptic curve with a triple pole at one point and a zero of at least order 3 at another point has exactly a triple zero there and nothing else in its divisor.

Since $\mathscr{I}_Q^3\mathscr{I}_e^{-3}$ has been proved to be trivial on E, it follows that $3[Q] = e$ in $E(S)$, so Q is a section of $E[3]$. Being disjoint from e and $\pm P$, it follows that (P,Q) is a full level-3 structure on E. The chain of arguments leading up to the special form given in the statement of the lemma show that there are no nontrivial changes of the Weierstrass coordinates which preserve the special form of the elliptic curve E and the points P and Q with $y - x - B$ lying in $\mathscr{I}_Q^3$. ∎

5. Functorial arguments

In this section, we explain how to use functorial techniques to establish properties of moduli schemes. We begin with smoothness.

Proposition 5.1. *For $N \geq 4$, assume representability of the functor assigning to every $\mathbf{Z}[1/N]$-scheme S the set of isomorphism classes of pairs $(E \to S, \phi)$ consisting of an elliptic curve E over S equipped with a full level-N structure. Assume moreover that the representing scheme $Y(N)$ is locally of finite type over $\mathbf{Z}[1/N]$. Then $Y(N) \to \mathbf{Z}[1/N]$ is smooth. In particular, this map is flat.*

For $N = 3, 4$ we see by inspection of the construction of $Y(N)$ that it is even affine. Likewise, in general $Y(N)$ will be affine of finite type by construction. But such affineness is not relevant to the proof below. Amusingly, Grothendieck even discovered a functorial criterion for a map between locally noetherian schemes to be locally of finite type! This can be used to prove the "locally finite type" property of $Y(N)$ over $\mathbf{Z}[1/N]$ by functorial considerations (assuming this scheme exists and is locally noetherian). However, that is a somewhat silly argument because although the construction of moduli schemes rarely tells us anything useful about its properties, at least the "finite type" property will always be clear from the construction.

Proof. By the functorial criterion for smoothness, it suffices to prove that if A is an artin local ring over $\mathbf{Z}[1/N]$ and if $A_0 = A/I$ for an ideal $I \subset \mathfrak{m}_A$ with $I^2 = 0$, then $Y(N)(A) \to Y(N)(A_0)$ is surjective. In other words, given an elliptic curve E_0 over A_0 and a full level-N structure ϕ_0 on E_0, we seek to construct a pair (E, ϕ) over A such that its mod-I reduction $(E, \phi) \bmod I = (E_{A_0}, \phi_{A_0})$ obtained via *base change* along $\operatorname{Spec} A_0 \to \operatorname{Spec} A$ is isomorphic to (E_0, ϕ_0). (Recall that the very definition of the contravariant functor represented by $Y(N)$ is via *base change* on pairs (E, ϕ), so we really are computing the map $Y(N)(A) \to Y(N)(A_0)$ correctly in terms of the functor of points of $Y(N)$.) In more concrete terms, we have to lift E_0 to an elliptic curve E over A, and then lift $\phi_0 : (\mathbf{Z}/N\mathbf{Z})^2_{A_0} \simeq E_0[N]$ to an A-group isomorphism $\phi : (\mathbf{Z}/N\mathbf{Z})^2_A \simeq E[N]$. Strictly speaking, we just need to find *some* E lifting E_0 for which such a ϕ lifting ϕ_0 exists. But in the present circumstances we will be lucky: it turns out that such a ϕ will exist for any E. In more general moduli problems, when proving smoothness one sometimes needs to be more judicious in the choice of initial step of a lifting process.

Here is how to build (E, ϕ) over A lifting (E_0, ϕ_0). Since A_0 is local, E_0 admits a Weierstrass model over A_0. Now lift all of the coefficients to A. This gives a Weierstrass cubic, and its discriminant Δ is a unit in A since the reduction Δ_0 in A_0 is a unit. Thus, we have lifted E_0 to an elliptic curve E over A. (For higher genus there is an analogue of this step, but it requires serious work in deformation theory and the vanishing of degree-2 coherent cohomology on curves over a field.) Now consider $E[N]$. Since $N \in A^\times$ (i.e., A is a $\mathbf{Z}[1/N]$-algebra), $E[N]$ is a finite étale A-group. But then by the functorial property for étale morphisms applied to $E[N] \to \operatorname{Spec} A$ it follows that the reduction map $E[N](A) \to E[N](A_0) = E_0[N](A_0)$ is *bijective*. Hence, ϕ_0 (viewed as an ordered pair of elements in $E_0[N](A_0)$) *uniquely lifts* to some $\phi : (\mathbf{Z}/N\mathbf{Z})^2_A \to E[N]$ over A. Moreover, this latter A-group map is a full level-N structure (i.e., an isomorphism) because the "finite étale" property of both sides reduces it to a problem on geometric fibers: there is just one geometric fiber (since A is artin local), and it coincides with the one over A_0, where the isomorphism property is inherited from ϕ_0. ∎

Corollary 5.2. *With hypotheses as in Proposition* 5.1*, the fibers of the map $Y(N) \to \operatorname{Spec} \mathbf{Z}[1/N]$ have pure dimension* 1*.*

Proof. The map $Y(N) \to \operatorname{Spec} \mathbf{Z}[1/N]$ is surjective, since over an algebraically closed field of characteristic not dividing N there are elliptic curves, and on any such elliptic curve we can impose a full level-N structure. Thus, all fibers are non-empty. The problem is to prove that if k is an algebraically closed field of characteristic not dividing N and if $y \in Y(N)(k) = Y(N)_k(k)$ then the tangent space to $Y(N)_k$ at y is 1-dimensional over k.

For *any* k-scheme Y locally of finite type and any $y \in Y(k)$, the tangent space to Y at y is the fiber of $Y(k[\epsilon]) \to Y(k)$ over y as a set, but we need to encode the k-linear structure in terms of the functor of points of Y on the category of k-algebras too (if we are to correctly compute the k-dimension by functorial

methods when $Y = Y(N)_k$). The k-action on the tangent space to Y at a k-point y is through functoriality applied to k-scaling on $k[\epsilon]$ (as a k-algebra): $c.(a + b\epsilon) = a + bc\epsilon$. (Check!) Likewise, the additive structure comes from applying the functor of points of Y to the k-algebra map

$$k[\epsilon] \times_k k[\epsilon] = k[\epsilon, \epsilon']/(\epsilon^2, {\epsilon'}^2, \epsilon\epsilon') \to k[\epsilon]$$

defined by $(\epsilon, 0), (0, \epsilon) \mapsto \epsilon$ (i.e., $a + b\epsilon + c\epsilon' \mapsto a + (b + c)\epsilon$). That it, we have the map of sets

$$Y(k[\epsilon]) \times_{Y(k)} Y(k[\epsilon]) \simeq Y(k[\epsilon] \times_k k[\epsilon]) \to Y(k[\epsilon])$$

over $Y(k)$ (where the isomorphism goes naturally from right to left!), and on y-fibers it induces addition on the fiber $\mathrm{Tan}_y(Y)$. (Check!)

Taking $Y = Y(N)_k$, we can now read off the k-vector space $\mathrm{Tan}_y(Y(N)_k)$ at a point $y = (E_0, \phi_0)$ over k in terms of the moduli functor of full level-N structures. To carry out the calculation, we first compute the underlying set in concrete terms, and then work out the k-linear structure on this set. The underlying set consists of isomorphism classes of pairs (E, ϕ) over $k[\epsilon]$ that lift (E_0, ϕ_0). Once we lift E_0 to E, the level structure ϕ lifting ϕ_0 always exists and is moreover unique: we saw this in the proof of Proposition 5.1 (taking $A \to A_0$ there to be $k[\epsilon] \to k$). Thus, the level structure just "comes along for the ride" and the problem is entirely one of deforming elliptic curves from k to $k[\epsilon]$. In fact, we do not even need to keep track of the identity section: a lift X of E_0 to a $k[\epsilon]$-curve makes $X(k[\epsilon]) \to X(k) = E_0(k)$ surjective due to the smoothness of X, so we can pick $x \in X(k[\epsilon])$ lifting $e_0 \in E_0(k)$, thereby making an elliptic curve (X, x). But the key is that the choice of x *doesn't matter*: if $x' \in X(k[\epsilon])$ is another choice then by using the unique $k[\epsilon]$-group structure on (X, x) we define a translation by x' to make a $k[\epsilon]$-automorphism of X carrying x to x', and on the special fiber E_0 this is translation by $x'_0 = e_0$, so nothing happens there. Thus, the pair (X, x) up to isomorphism is independent of the choice of x, so we can just as well view the tangent space to (E_0, ϕ_0) as the set of isomorphism classes of flat deformations of E_0 over $k[\epsilon]$ as a "bare curve". The same goes for deformations to other artin local k-algebras with residue field k, such as $k[\epsilon] \times_k k[\epsilon]$.

Now it is a general fact that for a smooth finite type separated scheme over k, its set of isomorphism classes of flat deformations to $k[\epsilon]$ is naturally identifed with the set $\mathrm{H}^1(X, (\Omega^1_{X/k})^\vee)$. The basic idea is to describe such deformations in terms of Čech theory using vector fields (which is what $(\Omega^1_{X/k})^\vee$ encodes), but it is a bit of a digression and so we do not get into the explanation of that dictionary here. The point is that when one unravels how the identification is defined, it turns out that the k-linear structure as described above in terms of the functor of deformations to $k[\epsilon]$ really does become the natural k-linear structure on $\mathrm{H}^1(X, (\Omega^1_{X/k})^\vee)$. When X is a proper and geometrically connected smooth curve, this is Serre-dual to $\mathrm{H}^0(X, (\Omega^1_{X/k})^{\otimes 2})$, whose dimension is $3g - 3$ when $g \geq 2$ (by Riemann–Roch considerations), and 1 when $g = 1$ (since in such cases $\Omega^1_{X/k} \simeq \mathscr{O}_X$). Thus, in our setting with $Y(N)_k$, the tangent space at $y = (E_0, \phi_0)$ is 1-dimensional over k. ■

Even though the separatedness of $Y(N)$ will be clear from our construction of it later (it will even be affine), it is amusing that this can also be proved via functoriality:

Proposition 5.3. *With hypotheses as in Proposition* 5.1*, the map* $Y(N) \to \mathrm{Spec}\, \mathbf{Z}[1/N]$ *is separated.*

Proof. Since we assume the existence of $Y(N)$ as a locally noetherian scheme, so its diagonal $\Delta_{Y(N)/\mathbf{Z}[1/N]}$ is quasi-compact, to check separatedness we can use the valuative criterion with discrete valuation rings. That is, for any discrete valuation ring R over $\mathbf{Z}[1/N]$ (i.e., the residue field k has characteristic not dividing N) and its fraction field K, we claim that the natural map $Y(N)(R) \to Y(N)(K)$ corresponding to base change along $\mathrm{Spec}\, K \to \mathrm{Spec}\, R$ on pairs (E, ϕ) is *injective*. In other words, if (E, ϕ) and (E', ϕ') are two pairs over R such that there is an isomorphism $E_K \simeq E'_K$ carrying ϕ_K to ϕ'_K then we claim that there is also such an isomorphism over R.

By the Néronian property of elliptic curves (a special case of this property for abelian schemes), the given isomorphism of elliptic curves over K extends to one over R. Carrying ϕ' back through this isomorphism, it now suffices to check that if two full level-N structures on E coincide over K then they are equal. That is, if two R-group isomorphisms $(\mathbf{Z}/N\mathbf{Z})^2_R \simeq E[N]$ coincide over K, then we claim that they agree. But this is

clear: in terms of the coordinate rings as finite free R-modules, it just says that an $N^2 \times N^2$-matrix over R is determined by its effect over K. ■

We conclude with an interesting application to the j-map. Say we grant the existence of $Y(N)$ as a *finite type* $\mathbf{Z}[1/N]$-scheme. We have seen that it is separated and smooth, with all fibers over $\mathbf{Z}[1/N]$ non-empty of pure dimension 1. But the universal elliptic curve $E_N \to Y(N)$ yields a j-map $j_{E_N/Y(N)} : Y(N) \to \mathbf{A}^1_{\mathbf{Z}[1/N]}$. In Remark 4.2 we explicitly computed this for $N = 3$, and in principle our construction for $N = 4$ yields an explicit description in that case (though it is somewhat messy for $N = 3$ and very messy for $N = 4$). The question is this: is this map *finite*? (In particular, that would provide a proof of affineness of $Y(N)$, although our eventual construction of $Y(N)$ will be affine by inspection. It is nonetheless worthwhile to have a conceptual explanation for why it is affine!) This too can be elegantly answered in the affirmative by functorial consideration, and its power is appreciated by recognizing that even in the "explicit" case $N = 3$ such finiteness is not at all obvious from staring at the explicit formulas.

Theorem 5.4. *If $Y(N)$ exists as a finite-type $\mathbf{Z}[1/N]$-scheme then $j_{E_N/Y(N)} : Y(N) \to \mathbf{A}^1_{Z[1/N]}$ is finite. Moreover, this map is flat.*

Proof. Once it is proved that $j = j_{E_N/Y(N)}$ is finite, on geometric fibers over $\operatorname{Spec} \mathbf{Z}[1/N]$ is is a finite map between smooth schemes of pure dimension 1 and hence is *flat* between such geometric fibers. Then the fibral flatness criterion from HW8 implies the flatness of j (as the source and target of j are $\mathbf{Z}[1/N]$-flat: for the source this follows from the established smoothness, which we proved via the functorial smoothness criterion, which did not "explicitly" involve flatness at the outset).

It remains to prove the finiteness of the morphism j. We will prove that it is proper and quasi-finite (so finiteness then follows via Zariski's Main Theorem). Since j is finite type (being a map between finite type $\mathbf{Z}[1/N]$-schemes), its quasi-finiteness is entirely a problem in terms of geometric points: we have to check that for any algebraically closed field k of characteristic not dividing N and any $j_0 \in k$, there are at most finitely many isomorphism classes of pairs (E, ϕ) over k such that $j(E) = j_0$. But over an algebraically closed field we know from the classical theory that $j(E)$ determines E up to isomorphism, and that all j-invariants do occur. So we fix an elliptic curve E_0 over k with j-invariants j_0, and the problem is to prove that there are only finitely many $\mathrm{Aut}(E_0)$-orbits on the set of full level-N structures on E_0. Even better, there are only finitely many such level structures, regardless of the $\mathrm{Aut}(E_0)$-action. This proves the quasi-finiteness of the j-morphism.

Finally, we prove that j is proper. We already know that $Y(N)$ is separated, so j is at least separated and finite type. By the valuative criterion for properness, it suffices to prove that for any discrete valuation ring R over $\mathbf{Z}[1/N]$ with fraction field K and any $j_0 \in \mathbf{A}^1_{\mathbf{Z}[1/N]}(R) = R$ and pair (E_η, ϕ_η) over K with $j(E_\eta) = j_0$, there exists a pair (E, ϕ) over R with $j(E) = j_0$ and $(E, \phi)_K \simeq (E_\eta, \phi_\eta)$.

For any local extension $R \to R'$ of discrete valuation rings and corresponding extension $K \to K'$ of fraction fields, it is easy to check that $Y(R') \cap Y(K) = Y(R)$ for any separated scheme Y. It follows that in the proof of the valuative criterion for separatedness, we may always replace R with R'. In particular, we may restrict our attention to complete R, and we can replace it with a finite extension later on if we wish. Since $j(E_\eta) = j_0 \in R$, E_η has potentially good reduction. Thus, passing to a finite extension of R (and of K), we can assume that E_η has good reduction; that is, it extends to an elliptic curve E over R! Of course, the element $j(E) \in R \subset K$ is $j(E_K) = j(E_\eta) = j_0$. Thus, it suffices to show that the full level-N structure ϕ_η on $E_K = E_\eta$ extends to one on E. The existence of ϕ_η implies that $E[N]_K = E_K[N]$ is a constant K-group (associated to $(\mathbf{Z}/N\mathbf{Z})^2$), and the Néronian property of E implies that $E(R) = E(K) = E_K(K)$, so $E[N](R) = E(R)[N] = E_K[N](K) = (\mathbf{Z}/N\mathbf{Z})^2$ via ϕ_η. Thus, we get an R-group homomorphism

$$\phi : (\mathbf{Z}/N\mathbf{Z})^2_R \to E[N]$$

that recovers the isomorphism ϕ_η over K, and so it remains to show that ϕ must be an isomorphism.

But R is a $\mathbf{Z}[1/N]$-algebra, so $E[N]$ is a finite étale R-scheme. Hence, as we saw in class, any section to $E[N] \to \operatorname{Spec} R$xsplits off as a clopen subscheme. The map ϕ assigns to any $(i, j) \in (\mathbf{Z}/N\mathbf{Z})^2$ a connected component $\operatorname{Spec} R$ of $E[N]$, and two such components are visibly distinct when their K-points are distinct in $E[N](K)$. We conclude that ϕ corresponds to a collection of N^2 pairwise distinct connected components,

and R-rank considerations for $E[N] \to \operatorname{Spec} R$ show that there is no room for anything else to be left over. Thus, ϕ is an isomorphism. ■

Another important geometric problem with moduli spaces is that of identifying the connected components. For this we cannot get by via functorial techniques. We will need to bring in two entirely new ideas: compactification and comparison with the complex-analytic theory. More on this later in the course.