Math 248B. Classical analytic modular curves

1. Motivation

In class we proved that for any $N \geq 3$ and $\zeta \in \mu_N^\times(\mathbf{C})$, the functor $[\Gamma(N)\text{-str}]^\zeta$ of isomorphism classes of $\Gamma(N)$-structures with Weil pairing ζ is representable. A representing object was constructed by a quotient process, which we now review.

Consider a universal H_1-trivialized pair $(\mathfrak{E} \to \mathfrak{M}, \phi)$. An explicit model is given by the Weierstrass family $\mathscr{E} \to \mathbf{C} - \mathbf{R}$ equipped with its H_1-trivialization via the ordered homology basis $\{\tau, 1\}$ of $\mathrm{H}_1(\mathscr{E}_\tau, \mathbf{Z}) = \Lambda_\tau = \mathbf{Z}\tau \oplus \mathbf{Z} \subset \mathbf{C}$ on the fiber over each $\tau \in \mathbf{C} - \mathbf{R}$. We prefer to think in terms of an "abstract" universal pair $(\mathfrak{E} \to \mathfrak{M}, \phi)$ to clarify matters, but the explicit Weierstrass family is convenient to keep in mind. Upon fixing a choice of $i = \sqrt{-1} \in \mathbf{C}$, the source and target of the universal isomorphism $\phi : \mathbf{Z}^2 \times \mathfrak{M} \simeq \underline{\mathrm{H}}_1(\mathfrak{E}/\mathfrak{M})$ have natural $\mathbf{Z}$-valued symplectic forms: the determinant pairing on the left side, and the fibral i-oriented intersection form on the right side. By inspection of the explicit analytic model over $\mathbf{C} - \mathbf{R}$, we see that $\mathfrak{M}$ has two connected components: on one component ϕ respects the two pairings, and on the other component it fails to be compatible (there is a universal sign discrepancy). Indeed, the i-oriented intersection form on $\mathrm{H}_1(\mathbf{C}/\Lambda_\tau, \mathbf{Z})$ carries the ordered homology basis $(\tau, 1)$ to 1 if $\tau \in \mathfrak{h}_{-i}$ and to -1 if $\tau \in \mathfrak{h}_i$.

Define $\mathfrak{M}_i$ to be the connected component over which ϕ carries the determinant pairing to the $-i$-oriented intersection form; note the sign. (For the Weierstrass family we have $\mathfrak{M}_i = \mathfrak{h}_i$.) The natural left action by $\mathrm{GL}_2(\mathbf{Z})$ on $(\mathfrak{E} \to \mathfrak{M}, \phi)$ swaps the two connected components of $\mathfrak{M}$, with $\mathrm{SL}_2(\mathbf{Z})$ the stabilizer of each component. In particular, $\mathrm{SL}_2(\mathbf{Z})$ has a natural left action on the restriction $(\mathfrak{E}_i \to \mathfrak{M}_i, \phi_i)$ over $\mathfrak{M}_i$, so we get a left action by the subgroup $\Gamma(N) := \ker(\mathrm{SL}_2(\mathbf{Z}) \to \mathrm{SL}_2(\mathbf{Z}/N\mathbf{Z}))$. In class we saw that for $N \geq 3$, this action on $\mathfrak{M}_i$ is properly discontinuous. The action of $\Gamma(N)$ on $\mathfrak{E}_i$ covering the action on $\mathfrak{M}_i$ is *equivariant* for the full level-N structure on $\mathfrak{E}_i[N] = \underline{\mathrm{H}}_1(\mathfrak{E}_i/\mathfrak{M}_i)$ mod N given by mod-N reduction of ϕ_i so this is also properly discontinuous. This ensures that there is a good notion of analytic quotient by these actions of $\Gamma(N)$ (as discussed in the handout "$\mathrm{GL}_2(\mathbf{Z})$-action and modular forms").

Passing to the quotient by $\Gamma(N)$ was seen to give an elliptic curve $\Gamma(N)\backslash\mathfrak{E}_i \to \Gamma(N)\backslash\mathfrak{M}_i$ equipped with a full level-N structure that has fibral Weil pairing $\zeta_{N,i} = e^{2\pi i/N}$, and that moreover this is *universal*; i.e., it represents the moduli problem $[\Gamma(N)\text{−str}]^{\zeta_{N,i}}$. This universal pair

$$(E_{N,\zeta_{N,i}} \to Y_{\zeta_{N,i}}(N), (P_{\zeta_{N,i}}, Q_{\zeta_{N,i}}))$$

was seen to yield a universal object for each the functor $[\Gamma(N)\text{−str}]^\zeta$ by using the same elliptic curve and keeping $Q_{\zeta_{N,i}}$ unchanged but multiplying $P_{\zeta_{N,i}}$ by $r \in (\mathbf{Z}/N\mathbf{Z})^\times$ where $\zeta = \zeta_{N,i}^r$. In this way, we proved that all of the functors $[\Gamma(N)\text{-str}]^\zeta$ are representable when $N \geq 3$; we write $(E_\zeta \to Y_\zeta(N), (P_\zeta, Q_\zeta))$ to denote a universal object for each $\zeta \in \mu_N^\times(\mathbf{C})$. The aim of this handout is to use the representability of every $[\Gamma(N)\text{-str}]^\zeta$ to deduce many other representability results.

Remark 1.1. There are many explicit choices that we could have made for the universal N-torsion basis with Weil pairing ζ on the explicit family of elliptic curves $\Gamma(N)\backslash\mathfrak{E}_i \to \Gamma(N)\backslash\mathfrak{M}_i$. More specifically, given one universal pair $(E_\zeta \to Y_\zeta(N), (P_\zeta, Q_\zeta))$ we can make many others with the same underlying elliptic curve by simply applying an element of $\mathrm{SL}_2(\mathbf{Z}/N\mathbf{Z})$ to (P_ζ, Q_ζ). This corresponds to the fact that $\mathrm{SL}_2(\mathbf{Z}/N\mathbf{Z})$ acts on the functor $[\Gamma(N)\text{-str}]^\zeta$, and reminds us that it is best to generally not think about universal objects in terms of their explicit construction but rather in terms of their universal property.

Of course, knowing explicit models is useful too! For instance, to prove that the base of a universal object $(\mathfrak{E} \to \mathfrak{M}, \phi)$ for the H_1-trivialized moduli problem has exactly two connected components, distinguished by comparing the determinant form on $\mathbf{Z}^2$ and the i-oriented intersection form on $\underline{\mathrm{H}}_1(\mathfrak{E}/\mathfrak{M})$ (for a fixed choice of $i \in \mathbf{C}$), we simply stare at the explicit construction and use our knowledge of the connected components of $\mathbf{C} - \mathbf{R}$. In the handout "$\mathrm{GL}_2(\mathbf{Z})$ and modular forms" we gave another proof via considerations with Lie groups and especially the connectedness of $\mathrm{SL}_2(\mathbf{R})$. Whether using the viewpoint of complex geometry or Lie groups, the only known proofs that the i-oriented H_1-trivialized moduli problem has a connected moduli space are by inspecting a construction. This is not a minor issue, since *all* known connectedness results for modular curves in the algebraic theory, *even in positive characteristic*, ultimately rest on the connectedness of the i-oriented H_1-trivialized moduli space.

2. The full level-N problem

We will be interested in studying moduli problems defined by "level-N" structures on elliptic curves over complex manifolds, and everything will ultimately be related to the full level-N moduli problem. Thus, we first use our work on the refinements with fixed Weil pairing to construct a universal object for the full level-N problem for $N \geq 3$.

Theorem 2.1. *For $N \geq 3$ and $\zeta \in \mu_N^\times(\mathbf{C})$, let $(E_\zeta \to Y_\zeta(N), (P_\zeta, Q_\zeta))$ be universal for $[\Gamma(N)\text{-str}]^\zeta$. The elliptic curve*

$$E_N = \coprod_\zeta E_\zeta \to \coprod_\zeta Y_\zeta(N) =: Y(N)$$

equipped with the full level-N structure (P_N, Q_N) restricting to (P_ζ, Q_ζ) over $Y_\zeta(N)$ for each ζ is universal for $[\Gamma(N)\text{-str}]$.

Proof. Let $E \to M$ be an elliptic curve over a complex manifold, and let (P, Q) be a full level-N structure. We seek to prove the existence and uniqueness of a cartesian diagram of elliptic curves

$$\begin{tikzcd}
E \arrow[r] \arrow[d] & E_N \arrow[d] \\
M \arrow[r, "h"'] & Y(N)
\end{tikzcd}$$

pulling (P_N, Q_N) back to (P, Q). We saw in class that the Weil pairing $\langle P(m), Q(m)\rangle_{E_m, N} \in \mu_N^\times(\mathbf{C})$ is locally constant in m. In other words, we get a unique decomposition $M = \coprod M_\zeta$ such that the restriction of $(E, (P, Q))$ over M_ζ has Weil pairing ζ on all fibers. In view of the functoriality of Weil pairings with respect to isomorphisms, if h is to exist then it must carry M_ζ into $Y_\zeta(N)$. Thus, to solve our problem it suffices to work over each M_ζ separately and replace $(E_N \to Y(N), (P_N, Q_N))$ with $(E_\zeta \to Y_\zeta(N), (P_\zeta, Q_\zeta))$. But this reduces us to to the case of $\Gamma(N)$-structures with fibral Weil pairing ζ, so we are done! ■

Remark 2.2. For the reader who knows the concept of "open subfunctor" what is going on in the above proof is that the decomposition $M = \coprod M_\zeta$ shows that the functor $[\Gamma(N)\text{-str}]$ is covered by a "disjoint union of open subfunctors" $[\Gamma(N)\text{-str}]^\zeta$. Rather generally, when a set-valued functor F on the category of complex manifolds (or schemes, or topological spaces, etc.) is covered by open subfunctors F_j then F is representable if and only every F_j is representable, with a representing object for F given by a suitable gluing of representing objects for the F_j (with this gluing a disjoint union when $F_j \cap F_{j'} = \emptyset$ inside of F whenever $j \neq j'$). This principle underlies many representability constructions via gluing, such as for Hilbert schemes (using the disjoint covering by open subfunctors arising from Hilbert polynomials), projective spaces, Grassmannians, and blow-ups.

If we write full level-N structures as pairs $(E \to M, \phi)$ where $\phi : (\mathbf{Z}/N\mathbf{Z})^2 \times M \to E[N]$ is an isomorphism of M-groups, then there is a natural left action of $\mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$ on the functor $[\Gamma(N)\text{-str}]$ via $\gamma.(E, \phi) = (E, \phi \circ \gamma^t)$. The effect of the γ-action on the μ_N-valued fibral Weil pairing is raising to the $\det \gamma$-power, so this action carries the subfunctor $[\Gamma(N)\text{-str}]^\zeta$ to the subfunctor $[\Gamma(N)\text{-str}]^{\zeta^{\det\gamma}}$ for each $\zeta \in \mu_N^\times(\mathbf{C})$. In particular, the action of $\mathrm{SL}_2(\mathbf{Z}/N\mathbf{Z})$ preserves these subfunctors, and for $N \geq 3$ this action is easy to describe on the explicit representing objects derived from the Weierstrass family $\mathscr{E} \to \mathbf{C} - \mathbf{R}$: do nothing to the level-N structure and act on $\Gamma(N)\backslash\mathscr{E}_i \to \Gamma(N)\backslash\mathfrak{h}_i$ via $\tau \mapsto (a\tau + b)/(c\tau + d)$ on the base $\mathfrak{h}_i$ and via $z \mapsto z/(c\tau + d)$ as an isomorphism $\mathbf{C}/\Lambda_\tau \simeq \mathbf{C}/\Lambda_{[\gamma](\tau)}$ between fibers, where $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbf{Z})$ is a lift of $\gamma \in \mathrm{SL}_2(\mathbf{Z}/N\mathbf{Z})$.

However, the effect of $\gamma \in \mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$ requires a bit more care to describe in general, when we allow $\det \gamma \neq 1$, because $\mathrm{GL}_2(\mathbf{Z}) \to \mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$ is *not* surjective (in contrast with SL_2). To explain this, we will use a $(\mathbf{Z}/N\mathbf{Z})^\times$-action on the full level-N moduli problem, as follows. For any $r \in (\mathbf{Z}/N\mathbf{Z})^\times$, let $\langle r\rangle = \left(\begin{smallmatrix} r & 0 \\ 0 & 1 \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$ (so $\det\langle r\rangle = r$). The effect of $\langle r\rangle$ on the full level-N functor is given by

$(E,(P,Q)) \mapsto (E,(rP,Q))$. On the universal object $(E_N \to Y(N),(P_N,Q_N))$, this corresponds to doing nothing to the elliptic curve $E_N \to Y(N)$ but replacing (P_N,Q_N) with (rP_N,Q_N). Equivalently, if we fix a representing object $(E_{\zeta_0} \to Y_{\zeta_0}(N),(P_{\zeta_0},Q_{\zeta_0}))$ for $[\Gamma(N)\text{-str}]^{\zeta_0}$ for one $\zeta_0 \in \mu_N^\times(\mathbf{C})$ and naturally identify

$$\coprod_r (E_{\zeta_0} \to Y_{\zeta_0}(N),(rP_{\zeta_0},Q_{\zeta_0}))$$

as universal for $[\Gamma(N)\text{-str}]$ then $\langle r\rangle$ simply permutes the connected components according to the rth-power map on $\mu_N^\times(\mathbf{C})$. (This is easily visualized for the explicit analytic model derived from the Weierstrass family over $\mathfrak{h}_i$ when we use $\zeta_0 = e^{2\pi i/N}$.)

Now for any $\gamma \in \mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$, we write

$$\gamma = \gamma'\langle\det\gamma\rangle,$$

so $\gamma' \in \mathrm{SL}_2(\mathbf{Z}/N\mathbf{Z})$. Then the effect of γ on an explicit universal object for $[\Gamma(N)\text{-str}]$ obtained from $\mathscr{E} \to \mathbf{C}-\mathbf{R}$ is given in two steps: the effect of $\langle\det\gamma\rangle$ (which is easy) and the effect of a lift to $\mathrm{SL}_2(\mathbf{Z})$ of $\gamma' \in \mathrm{SL}_2(\mathbf{Z}/N\mathbf{Z})$ (which can be a bit "ugly").

3. Analytic quotients in dimension 1

We now make a digression to discuss quotients by discrete group actions in a broader sense than was considered in the handout "$\mathrm{GL}_2(\mathbf{Z})$-action and modular forms". Recall that the action by a group Γ on a Hausdorff topological space X is called *discontinuous* if the stabilizer $\Gamma_x = \{\gamma \in \Gamma \mid \gamma(x) = x\}$ at each $x \in X$ is finite and there exists an open $U \subset X$ around x such that $\gamma(U) \cap U \neq \emptyset$ if and only if $\gamma \in \Gamma_x$. (If moreover every Γ_x is trivial then the action is called *properly discontinuous.*) In the earlier handout we saw that for any Lie group G with finite compact group and any maximal compact subgroup K in G, the left action on G/K by a discrete subgroup Γ of G is always discontinuous, and is properly discontinuous if and only if Γ is torsion-free. This was used to make sense of an *analytic* quotient $\Gamma\backslash\mathfrak{h}_i$ for a torsion-free discrete subgroup Γ in $\mathrm{SL}_2(\mathbf{R})$. But what happens when the action is merely discontinuous (i.e., the finite stabilizers Γ_x may be nontrivial)?

In this section, we wish to take up the task of making sense of quotients $\Gamma\backslash X$ for the discontinuous action of a group Γ on a Hausdorff complex manifold X of pure dimension 1. (The case of higher-dimensional X is important, but in that generality one really has to work with complex-analytic spaces, because it is too restrictive to expect the quotient to exist as a manifold; the same problem arises in the algebro-geometric case for the action by a finite group on a smooth quasi-projective variety over a field.) In books on classical modular forms this is typically carried out in special cases when Γ is discrete in $\mathrm{GL}_2(\mathbf{R})$ acting on (a connected component of) $\mathbf{C}-\mathbf{R}$, exploiting special features of that situation. We will now explain how to make sense of $\Gamma\backslash X$ in a useful way *without* any crutch of half-planes and linear-fractional transformation formulas.

Proposition 3.1. *Let Y be a Hausdorff complex manifold of pure dimension* 1 *equipped with a discontinuous action by a group Γ.*

(1) *The topological quotient $\Gamma\backslash Y$ is Hausdorff, and the mapping $\pi : Y \to \Gamma\backslash Y$ is proper with finite fibers.*
(2) *On $\Gamma\backslash Y$ there is a unique analytic structure with respect to which π is a holomorphic, and this makes π initial among Γ-invariant holomorphic maps from Y to complex manifolds.*

Proof. This problem is local over the topological quotient $\Gamma\backslash Y$, so by discontinuity of the action we may reduce to the case when Γ is finite of size $n > 0$ and fixes a point $y \in Y$. We may then replace Y with a Γ-stable connected open set containing y so that Y is connected. Thus, by analytic continuation (and holomorphicity of the Γ-action), any $\gamma \in \Gamma$ that acts trivially on a small open around y must act trivially on all of Y. That is, if we replace Γ with its image in $\mathrm{Aut}(Y)$ then we can arrange that not only does Γ act faithfully on Y but that it also does so on any Γ-stable non-empty open set in Y. In particular, the faithfulness is not lost under shrinking around y.

Let t be a local holomorphic coordinate on a Γ-stable open set $U \subset Y$ around y such that $t(y) = 0$, and replace U with the connected component of y so that U is connected. Observe that on any non-empty open set in U, distinct elements of Γ have distinct actions.

Clearly $f = \mathrm{N}_\Gamma(t) := \prod_\Gamma (t \circ \gamma)$ is a Γ-invariant function on U with a zero of order exactly n at y. Hence, by shrinking U we can arrange that $f = z^n$ for a holomorphic coordinate z on U near y with $z(y) = 0$, so $(z \circ \gamma)^n = f \circ \gamma = f = z^n$ for all $\gamma \in \Gamma$. This implies $z \circ \gamma = \zeta_\gamma z$ for some $\zeta_\gamma \in \mu_n(\mathbf{C})$, and since $z \circ \gamma \neq z \circ \gamma'$ for distinct $\gamma, \gamma' \in \Gamma$ we have that $\gamma \mapsto \zeta_\gamma$ is a homomorphism $\Gamma \hookrightarrow \mu_n(\mathbf{C})$. Moreover, this is *injective* due to the arranged faithfulness of the action near y, yet $n = \#\Gamma$, so $\Gamma \hookrightarrow \mu_n(\mathbf{C})$ is an equality. In other words, by replacing t with z and Y with U (as we may) we arrange that U is open in $\mathbf{C}$ around $y = 0$ and stable under the scaling action by $\Gamma = \mu_n(\mathbf{C})$. Then it is clear that the nth-power map $U \to \mathbf{C}$ is a proper map onto its open image U' and has fibers of degree n, with $U \to U'$ an analytic quotient for the Γ-action on U.

The uniqueness of the analytic structure on $\Gamma\backslash Y$ follows from the universal quotient property of the analytic structure we have constructed and the fact that a bijective holomorphic map between open sets in $\mathbf{C}$ is an analytic isomorphism. ■

4. Some quotient formalism

For a subgroup $\Gamma \subset \mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$, in Exercise 4 of HW4 we defined the concept of a Γ-*structure* α on an elliptic curve E over a complex manifold M, as well as a notion of *isomorphism* for pairs $(E \to M, \alpha)$. We emphasize that Γ comes *equipped* with its embedding into $\mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$; e.g., if $\Gamma = 1$ then N is part of the data too. In what follows we will assume the reader has done part (i) of that exercise, as well as the examples given in parts (ii) and (iii). The existence of the moduli space for full level-N structures when $N \geq 3$ will now be used to make moduli spaces for functors of isomorphism classes of elliptic curves equipped with Γ-structure.

Example 4.1. When $\Gamma = 1$, it is immediate from the definitions that in this case a Γ-structure is the same thing as a full level-N structure.

By part (i) of Exercise 4 of HW4 we know that elliptic curves equipped with Γ-structure are rigid (i.e., admit no nontrivial automorphisms) if and only if Γ acts freely on $Y(N)$. Here is a more group-theoretic interpretation:

Proposition 4.2. *Let $\widetilde{\Gamma} \subset \mathrm{SL}_2(\mathbf{Z})$ denote the preimage of $\Gamma \cap \mathrm{SL}_2(\mathbf{Z}/N\mathbf{Z})$ under the surjective homomorphism $\mathrm{SL}_2(\mathbf{Z}) \to \mathrm{SL}_2(\mathbf{Z}/N\mathbf{Z})$. Elliptic curves equipped with Γ-structure are rigid if and only if $\widetilde{\Gamma}_{\mathrm{tor}} = 1$; i.e., $\widetilde{\Gamma}$ contains no nontrivial elements of finite order.*

Proof. This can be proved in a classical style by short but messy calculations with linear fractional transformations on $\mathbf{C} - \mathbf{R}$. We will give a longer but entirely conceptual proof using moduli-theoretic reasoning and general properties of connected Lie groups (such as $\mathrm{SL}_2(\mathbf{R})$), as this reveals the essentially group-theoretic nature of the problem and paves the way for similar results when GL_2 is replaced with other linear algebraic groups in generalizations of the theory of modular forms.

If $\gamma \in \Gamma$ fixes a point on $Y(N)$ then necessarily the element $\det \gamma \in (\mathbf{Z}/N\mathbf{Z})^\times$ is trivial, since the γ-action on $Y(N)$ permutes the connected components $Y_\zeta(N)$ according to the $\det \gamma$-power map on $\mu_N^\times(\mathbf{C})$. Thus, we may and do replace Γ with $\Gamma \cap \mathrm{SL}_2(\mathbf{Z}/N\mathbf{Z})$. Let $(\mathfrak{E} \to \mathfrak{M}, \phi)$ be universal for the H_1-trivialization moduli problem (this is just the Weierstrass family over $\mathbf{C} - \mathbf{R}$ in disguise). Fix a connected component $\mathfrak{M}_0$ of $\mathfrak{M}$, so (as we saw in the construction of $Y(N)$) the action of Γ on $Y_\zeta(N) = \Gamma(N)\backslash\mathfrak{M}_0$ is induced by the action of $\widetilde{\Gamma}$ on $\mathfrak{M}_0$. This latter action on $\mathfrak{M}_0$ has nothing to do with ζ.

By the handout "$\mathrm{GL}_2(\mathbf{Z})$-action and modular forms", the moduli-theoretic action of $\mathrm{GL}_2(\mathbf{Z})$ on $\mathfrak{M}$ extends to a moduli-theoretic action of $\mathrm{GL}_2(\mathbf{R})$ on $\mathfrak{M}$ via variations of complex structure on $\mathbf{R}^2$, and in particular we get a moduli-theoretic action of $\mathrm{SL}_2(\mathbf{R})$ on $\mathfrak{M}_0$. This is just the classical linear fractional action of G on connected components of $\mathbf{C} - \mathbf{R}$, for which it is classically well-known that the $\mathrm{SL}_2(\mathbf{R})$-action is transitive with maximal compact subgroup $\mathrm{SO}_2(\mathbf{R})$ as the stabilizer of i in each component. Near the end of that earlier handout, we gave a moduli-theoretic proof of these facts, without appealing to the Weierstrass family model or formulas with linear fractional transformations.

It is a general fact in the theory of Lie groups that for any transitive C^∞-action of a (paracompact) Lie group G on a (Hausdorff) C^∞- manifold X, if $x \in X$ is a point and $G_x \subset G$ denotes its (closed) stabilizer then $g \mapsto g.x$ induces a G-equivariant C^∞-isomorphism $G/G_x \simeq X$. In our setting, this recovers the classical

$\mathrm{SL}_2(\mathbf{R})$-equivariant isomorphism of $\mathrm{SL}_2(\mathbf{R})/\mathrm{SO}_2(\mathbf{R})$ onto a connected component of $\mathfrak{M}$ via the base point $\pm i$ in that component. Under this identification of each connected component of $\mathfrak{M}$ with the quotient G/K modulo the maximal compact subgroup K of $G = \mathrm{SL}_2(\mathbf{R})$, the G-action on $\mathfrak{M}$ is left multiplication. Hence, the same holds for the description of the action of the discrete subgroup $\Gamma_0 := \mathrm{SL}_2(\mathbf{Z})$ in G.

Now it suffices to prove that an element $\gamma \in \Gamma_0$ has a fixed point under left translation on G/K if and only if γ has finite order. This is a general fact for *any* connected Lie group G and compact subgroup K, as we now explain. The condition of γ fixing a coset gK is that $\gamma gK = gK$, which is to say $g^{-1}\gamma g \in K$, or equivalently $\gamma \in gKg^{-1}$. But all maximal compact subgroups of G are conjugate, so it is equivalent to say that γ lies in a compact subgroup of G. Since Γ_0 is discrete in G, its intersection with any compact subgroup of G is *finite*, so certainly if γ lies in a compact subgroup of G then it has finite order. Conversely, if γ has finite order then it generates a compact (even finite!) subgroup, and every compact subgroup of G lies in a maximal one. ■

Example 4.3. Taking $\Gamma = \{1\}$ in $\mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$, the rigidity of full level-N structures for $N \geq 3$ is a logical consequence of the purely group-theoretic fact that $\Gamma(N)$ is torsion-free when $N \geq 3$. Using parts (ii) and (iii) of Exercise 4 of HW4, we see that $\Gamma_1(N) \subset \mathrm{SL}_2(\mathbf{Z})$ contains no nontrivial torsion if and only if $N \geq 4$, whereas $\Gamma_0(N)$ always contains the nontrivial torsion element -1. Correspondingly, the $\Gamma_1(N)$-moduli problem is rigid when $N \geq 4$ but the $\Gamma_0(N)$-moduli problem is never rigid. There is no need to do computations with linear fractional transformations on $\mathfrak{h}_{\pm i}$ for any of this!

Our interest in the rigid case is due to:

Theorem 4.4. *Let $\Gamma \subset \mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$ be a subgroup such that all pairs (E, α) consisting of elliptic curves equipped with Γ-structures are rigid. The moduli problem of isomorphism classes of such pairs is represented by some $(E_\Gamma \to Y_\Gamma, \alpha_\Gamma)$, with Y_Γ Hausdorff of pure dimension 1, and the set of connected components of Y_Γ is naturally a principal homogeneous space for $(\mathbf{Z}/N\mathbf{Z})^\times/\det(\Gamma)$. In particular, Y_Γ is connected if and only if $\det : \Gamma \to (\mathbf{Z}/N\mathbf{Z})^\times$ is surjective.*

Proof. If N' is a positive multiple of N then the natural map $\mathrm{GL}_2(\mathbf{Z}/N'\mathbf{Z}) \to \mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$ is surjective (ultimately due to the analogue for SL_2), so if Γ' denotes the preimage of Γ in $\mathrm{GL}_2(\mathbf{Z}/N'\mathbf{Z})$ then it is easy to check that Γ'-structures on an elliptic curve $E \to M$ are "the same" as Γ-structures. Hence, we may and do assume $N \geq 3$, so the full level-N moduli problem is represented by some $(E_N \to Y(N), (P_N, Q_N))$.

Consider the natural left action of Γ on the $E_N \to Y(N)$ via the inclusion of Γ into $\mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$. By Exercise 4(i) in HW4, the rigidity hypothesis implies that the Γ-action on $Y(N)$ is free (so it is properly discontinuous, as Γ is finite and $Y(N)$ is Hausdorff), and hence the action on E_N is also properly discontinuous (as this "lies over" the action on $Y(N)$). Hence, the quotient

$$E_\Gamma := \Gamma\backslash E_N \to \Gamma\backslash Y(N) =: Y_\Gamma$$

makes sense as an elliptic curve, and by the very definition of "Γ-structure" this elliptic curve is equipped with a Γ-structure α_Γ obtained from the $\Gamma(N)$-structure on $E_N \to Y(N)$.

To prove that $(E_\Gamma \to Y_\Gamma, \alpha_\Gamma)$ is universal, consider any pair $(E \to M, \alpha)$ consisting of an elliptic curve E over a complex manifold M and a Γ-structure α on $E \to M$. We seek to prove the existence and uniqueness of a cartesian diagram of elliptic curves

$$\begin{tikzcd} E \arrow[r] \arrow[d] & E_\Gamma \arrow[d] \\ M \arrow[r] & Y_\Gamma \end{tikzcd}$$

such that α_Γ is pulled back to α. By the same argument we have seen several times in class, the rigidity hypothesis implies that the map along the top is uniquely determined by the map along the bottom (if such maps exist!). We will first prove the uniqueness of the map along the bottom in general, and then can work locally for existence.

For uniqueness, since a holomorphic map $M \to Y_\Gamma$ is determined by its effect on underlying sets, it suffices to show that as we vary through the points $y \in Y_\Gamma$, the fibers $(E_{\Gamma,y}, \alpha_{\Gamma,y})$ are pairwise non-isomorphic.

Suppose there is an isomorphism $\xi : E_{\Gamma,y} \simeq E_{\Gamma,y'}$ carrying $\alpha_{\Gamma,y}$ to $\alpha_{\Gamma,y'}$. Going back to the definition of "Γ-structure" when the base M is a point, the set of Γ-structures on a classical elliptic curve is the set of full level-N-structures taken up to Γ-action. Thus, we can choose full level-N structures ϕ on $E_{\Gamma,y}$ and ϕ' on $E_{\Gamma,y'}$ that respectively represent the Γ-orbits $\alpha_{\Gamma,y}$ and $\alpha_{\Gamma,y'}$. It follows that the full level-N structure $\xi^*(\phi')$ on $E_{\Gamma,y}$ is in the Γ-orbit of ϕ, so if $\widetilde{y}, \widetilde{y}' \in Y(N)$ respectively correspond to $(E_{\Gamma,y}, \phi)$ and $(E_{\Gamma,y'}, \phi')$ then $\widetilde{y}$ and $\widetilde{y}'$ lie in the same Γ-orbit on the *moduli space* $Y(N)$ (due to how the Γ-action on $Y(N)$ is *defined*). But then their images $y, y' \in \Gamma\backslash Y(N) = Y_\Gamma$ coincide, as desired. This finishes the proof of uniqueness of the desired cartesian diagram.

Now consider the problem of existence of the desired cartesian diagram. By the proved uniqueness, we may work locally on M for existence. Hence, by *definition* of Γ-structures in terms of global sections of a quotient sheaf (of sets), by working locally on M we may arrange that there is a full level-N-structure $\phi : (\mathbf{Z}/N\mathbf{Z})^2 \times M \simeq E[N]$ that induces α. Thus, we get a cartesian diagram

$$\begin{tikzcd} E \arrow[r] \arrow[d] & E_N \arrow[d] \\ M \arrow[r] & Y(N) \end{tikzcd}$$

pulling the universal full level-N structure back to ϕ. By construction of $E_\Gamma \to Y_\Gamma$ via a quotient process, the diagram

$$\begin{tikzcd} E_N \arrow[r] \arrow[d] & E_\Gamma \arrow[d] \\ Y(N) \arrow[r] & Y_\Gamma \end{tikzcd}$$

is cartesian and pulls α_Γ back to the Γ-structure on $E_N \to Y(N)$ induced by the universal full level-N structure. Hence, by concatenation of cartesian squares, existence is proved.

Finally, we check that the set of connected components of Y_Γ is a principal homogeneous space for $(\mathbf{Z}/N\mathbf{Z})^\times/\det(\Gamma)$. The action by $\gamma \in \mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$ on $Y(N) = \coprod_\zeta Y_\zeta(N)$ permutes the connected components $Y_\zeta(N)$ according to the $\det\gamma$-power map on $\mu_N^\times(\mathbf{C})$, and $\mu_N^\times(\mathbf{C})$ is a principal homogeneous space under $(\mathbf{Z}/N\mathbf{Z})^\times$ via the exponentiation $c.\gamma = \gamma^c$, so we are done. ■

Using (the solution to) Exercise 4(iii) in HW4, we obtain:

Corollary 4.5. *For $N \geq 4$, the moduli problem of points of exact order N on elliptic curves over complex manifolds is representable. For a choice of $i = \sqrt{-1} \in \mathbf{C}$, the representing object is given by the quotient of $\mathscr{E}^{(i)} \to \mathfrak{h}_i$ by the action of $\Gamma_1(N) \subset \mathrm{SL}_2(\mathbf{Z})$, taking the point of exact order N in $\mathscr{E}^{(i)}_\tau = \mathbf{C}/\Lambda_\tau$ to be $1/N \bmod \Lambda_\tau$ for every $\tau \in \mathfrak{h}_i$.*

Example 4.6. Fix $\zeta \in \mu_N^\times(\mathbf{C})$. Let's describe the classical Atkin-Lehner involution w_ζ of $Y_1(N)$ moduli-theoretically via an involution on the $\Gamma_1(N)$-moduli problem, and then related it to "explicit formulas" in terms of an explicit analytic model for the universal $\Gamma_1(N)$-structure.

Consider an elliptic curve $E \to M$ and $\Gamma_1(N)$-structure $P \in E[N](M)$ generating an M-subgroup $C = \langle P \rangle$. The Weil pairing on $E[N]$ is fiberwise perfect and induces an identification of $E[N]/C$ with the Cartier dual $\mu_N \times M$ of $C = \mathbf{Z}/N\mathbf{Z} \times M$ (using the generator P for this final equality). Using our choice of $\zeta \in \mu_N^\times(\mathbf{C})$ as a basis of μ_N, we thereby identify $E[N]/C$ with $(\mathbf{Z}/N\mathbf{Z}) \times M$ via a unique $Q \in (E[N]/C)(M)$. (On fibers, this corresponds to a unique point $Q(m) \in E_m[N]/C_m$ such that $\langle P(m), Q(m) \rangle_{E_m,N} = \zeta$; this condition make sense since the second variable in this pairing only matters modulo $C_m = \langle P(m) \rangle$.) The operation $w_\zeta : (E, P) \mapsto (E/\langle P \rangle, Q)$ is the involution we seek.

Why is it an involution? By rigidity this is a problem on fibers of the universal family, and to avoid total confusion caused by tracking the effect of isogenies on Weil pairings it is simplest to do a fibral calculation with an explicit analytic model. Fix $i = \sqrt{-1}$, so $\zeta = e^{2\pi i r/N}$ for some $r \in (\mathbf{Z}/N\mathbf{Z})^\times$. Take $(E, P) = (\mathbf{C}/\Lambda_\tau, 1/N)$ with $\tau \in \mathfrak{h}_i$, so $E/\langle P \rangle = \mathbf{C}/\Lambda_{N\tau}$ via multiplication by N on $\mathbf{C}$, in which $Q = r\tau \bmod \Lambda_{N\tau}$. Iterating the process yields $(\mathbf{C}/\Lambda_\tau, -1/N) \simeq (\mathbf{C}/\Lambda_\tau, 1/N) = (E, P)$ (using negation on $\mathbf{C}$), so we win.

Observe that $(\mathbf{C}/\Lambda_{N\tau}, r\tau) \simeq (\mathbf{C}/\Lambda_{-1/N\tau}, r/N)$ via multiplication by $1/N\tau$ on $\mathbf{C}$, and $(\mathbf{C}/\Lambda_{\tau'}, r/N) \simeq (\mathbf{C}/\Lambda_{[\delta_r](\tau')}, 1/N)$ via multiplication by $1/(c_r\tau + d_r)$ where $\delta_r := \left(\begin{smallmatrix} a_r & b_r \\ c_r & d_r \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbf{Z})$ is a lift of $\left(\begin{smallmatrix} 1/r & * \\ 0 & r \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbf{Z}/N\mathbf{Z})$. This calculation also shows that the effect of the involution w_ζ on the base $Y_1(N)$ of the universal family is induced by $\tau \mapsto [\delta_r](-1/N\tau)$ on $\mathfrak{h}_i$ when $\zeta = e^{2\pi i r/N}$ and we use the explicit analytic model $\Gamma_1(N)\backslash\mathscr{E}^{(i)} \to \Gamma_1(N)\backslash\mathfrak{h}_i$ with the N-torsion section $1/N$ on fibers.

When $r = \epsilon = \pm 1$, the "natural" choice of δ_r is $\left(\begin{smallmatrix} \epsilon & 0 \\ 0 & \epsilon \end{smallmatrix}\right)$; for other r the choice is a mess. Also, if we use a *different* universal $\Gamma_1(N)$-structure over $\Gamma_1(N)\backslash\mathfrak{h}_i$ (e.g., the same elliptic curve, but N-torsion section τ/N on fibers) then the "formula" for w_ζ will change! It is cleaner and more intrinsic to think about w_ζ in abstract moduli-theoretic terms rather than get hung up on explicit analytic models, though the explicit models are useful for some computations.

Example 4.7. If $N, N' \geq 1$ are relatively prime and $\Gamma \subset \mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$ and $\Gamma' \subset \mathrm{GL}_2(\mathbf{Z}/N'\mathbf{Z})$ are two subgroups then $\Gamma \times \Gamma' \subset \mathrm{GL}_2(\mathbf{Z}/NN'\mathbf{Z})$ is a subgroup. Clearly if Γ-structures are rigid then so are $\Gamma \times \Gamma'$-structures. For example, the so-called $\Gamma_1(N, N')$-moduli problem consists of triples (E, P, C) where $P \in E[N](M)$ has fiberwise exact order N and $C \subset E[N']$ is fiberwise cyclic of order N', and as long as $N \geq 4$ these are rigid. Thus, there is a moduli space $Y_1(N, N')$ and it is *connected.* For applications with Hecke operators this is of most interest when $N' = p$ is a prime not dividing N.

What is an explicit analytic model for $Y_1(N, N')$? It is given by the quotient of $\mathfrak{h}_i$ modulo the preimage in $\mathrm{SL}_2(\mathbf{Z})$ of the determinant-1 subgroup of $\Gamma \times \Gamma'$, and the fiber of the universal family over the coset of τ is given by $\mathbf{C}/\Lambda_\tau$ equipped with the point $1/N$ and the subgroup $\langle 1/N' \rangle$. Of course, there are a zillion other explicit analytic models over the same base (even with the same underlying family of elliptic curves!), corresponding to various other subgroups of $\mathrm{SL}_2(\mathbf{Z})$, such as using $\{\left(\begin{smallmatrix} * & 0 \\ * & * \end{smallmatrix}\right)\}$ for $\Gamma_0(N')$ and taking $\langle \tau/N' \rangle$ for the order-N' subgroup. It gets extremely confusing if these explicit analytic models are regarded as the basic objects of study, since we cannot easily see what is intrinsic. This is why the abstract moduli-theoretic viewpoint is superior: it forces us to focus on intrinsic structures when making definitions and constructions. Only for occasional calculations should we haul out a (conveniently chosen!) explicit analytic model.

For example, consider the moduli space $Y_1(N, N')$. There are canonical holomorphic maps $Y_1(N, N') \rightrightarrows Y_1(N)$ respectively given by the natural transformations of functors

$$\pi_1 : (E \to M, P, C) \mapsto (E \to M, P), \quad \pi_2 : (E \to M, P, C) \mapsto (E/C \to M, P \bmod C).$$

If we want to make these "explicit", we have to *specify* explicit analytic models for these moduli spaces. Let's use quotients of the Weierstrass family over $\mathfrak{h}_i$ by the subgroups $\Gamma_1(N, N') = \Gamma_1(N) \cap \Gamma_0(N')$ and $\Gamma_1(N)$, corresponding to the respective families whose fibers over τ are $(\mathbf{C}/\Lambda_\tau, 1/N, \langle 1/N' \rangle)$ and $(\mathbf{C}/\Lambda_\tau, 1/N)$. Thus, *in terms of these explicit analytic models*, π_1 is the canonical quotient map $\Gamma_1(N, N')\backslash\mathfrak{h}_i \to \Gamma_1(N)\backslash\mathfrak{h}_i$ whereas π_2 is induced by the "ugly" $\tau \mapsto [\delta_{1/N'}](N'\tau)$ because

$$(\mathbf{C}/(\Lambda_\tau + {N'}^{-1}\mathbf{Z}), 1/N) \simeq (\mathbf{C}/\Lambda_{N'\tau}, N'/N) \simeq (\mathbf{C}/\Lambda_{[\delta_{1/N'}](N'\tau)}, 1/N).$$

If we had used a different analytic model (e.g., taking the cyclic order-N' subgroup on the fiber over τ to be generated by τ/N') then we would obtain *entirely different* explicit analytic formulas for π_1 and π_2. So we really should not attach any intrinsic significance to such analytic formulas, but when making the passage to the algebro-geometric theory it will be important to check that *with suitable analytic models* we do recover constructions in the classical analytic theory.

5. Coarse moduli spaces

We finish with a discussion of what can be done when rigidity fails (such as for $\Gamma_0(N)$, or full level-N structures with $N < 3$). The basic idea is that if a set-valued contravariant functor F on a category C is not representable then we seek the "simplest" representable functor $h_M = \mathrm{Hom}_C(\cdot, M)$ to which F maps. In what follows, we write $*$ to denote the one-point complex manifold (with structure sheaf $\mathbf{C}$), so for any complex manifold M the set $\mathrm{Hom}(*, M)$ is naturally identified with the underlying set of M.

Definition 5.1. Let F be a set-valued functor on the category of complex manifolds. A *coarse moduli space* for F is a complex manifold $\mathscr{M}$ equipped with a natural transformation $\theta : F \to h_{\mathscr{M}}$ such that θ is initial (in the sense that any natural transformation $F \to h_X$ uniquely factors through θ via h_f for a unique $f : \mathscr{M} \to X$) and θ is bijective on $*$-valued points (i.e., $F(*) \to \mathscr{M}$ is bijective).

This definition is somewhat abstract, but in Proposition 5.2 we will describe it in more concrete terms. It is immediate from the definition that such a pair $(\mathscr{M}, \theta)$ is unique up to unique isomorphism if it exists, and that the condition of bijectivity on $*$-valued points is not necessary for such uniqueness. Rather, this bijectivity property is required to ensure that the underlying set of $\mathscr{M}$ and the meaning of the "coarse moduli spaces" property are accessible, as we now explain.

A good way to think about the meaning of the coarse moduli space property can be seen when $F(M)$ is the set of isomorphism classes of some kind of "structure" over M (such as an elliptic curve equipped with Γ-structure). In such cases $\mathscr{M}$ is identified with the set $F(*)$ of all "classical structures" and a natural transformation $T : F \to h_X$ is precisely a *functorial* assignment of a *holomorphic* map $T_\xi : M \to X$ to every "structure" $\xi \in F(M)$. Since maps of complex manifolds are determined by their effect on underlying sets, and the underlying set of a complex manifold is the set of maps from $*$, the coarse moduli space condition says exactly:

Proposition 5.2. *A complex manifold $\mathscr{M}$ is identified as a coarse moduli space for the functor F if and only if the set $\mathscr{M}$ is identified with the set $F(*)$ in such a way that for any $\xi \in F(M)$ the "classifying map" of sets $M \to \mathscr{M}$ carrying each $m \in M$ to the isomorphism class $\xi_m \in F(*) = \mathscr{M}$ is holomorphic.*

Proof. This is variant on the proof of Yoneda's Lemma, so it is left as an instructive exercise to the reader. ∎

The holomorphicity condition in this proposition is the real point; it is much stronger than just says that $\mathscr{M}$ is put in bijection with $F(*)$, and gives real meaning to the "analytic structure" on $F(*)$ obtained from $\mathscr{M}$. When a coarse moduli space $\mathscr{M}$ exists, there is generally *no* distinguished object in $F(\mathscr{M})$, and this set could well be empty!

Note that the viewpoint of coarse moduli spaces concerns morphisms *out* of the functor whereas the viewpoint of representing a functor concerns morphisms *into* the functor. Fortunately, Proposition 5.2 provides a viewpoint on the coarse moduli space that is close in spirit to the viewpoint of representability. It is an easy exercise to check that if F is represented by some $\mathscr{M}$ via an object $\xi \in F(\mathscr{M})$, then the isomorphism $F \simeq h_{\mathscr{M}}$ defined via ξ makes $\mathscr{M}$ a coarse moduli space. Thus, representability is a stronger condition on F than the existence of a coarse moduli space, and we often use the phrase "fine moduli space" as a synonym for "representing object" for a functor.

The concept of coarse moduli space is quite weak, and not at all well-suited to geometric categories where morphisms are not determined by their effect on composition with maps from a single object (as happens for the category of complex manifolds and the object $*$, or the category of reduced schemes of finite type over an algebraically closed field k and the object $\mathrm{Spec}(k)$). Also, when working in relative settings, the formation of a coarse space may not commute with base change whereas for representable functors on categories with enough fiber products this defect never occurs. The theory of stacks provides a much better notion than that of "coarse moduli spaces" in the absence of representability, but coarse moduli spaces are nonetheless useful (and are rediscovered in a new way when using stacks).

Example 5.3. If F admits a coarse moduli space $\mathscr{M}$ and F' admits a coarse moduli space $\mathscr{M}'$ then for any natural transformation $T : F \to F'$ there is a unique holomorphic map $f : \mathscr{M} \to \mathscr{M}'$ making the diagram of natural transformations

$$\begin{tikzcd}
F \arrow[r, "T"] \arrow[d, "\theta"'] & F' \arrow[d, "\theta'"] \\
h_{\mathscr{M}} \arrow[r, "f"'] & h_{\mathscr{M}'}
\end{tikzcd}$$

commute. On underlying sets, f is the map T on $*$-points. Hence, the content is that the map on $*$-points really is holomorphic.

Example 5.4. The functor of $\Gamma_0(N)$-structures (see Exercise 4(iii) on HW4) is not rigid, and we will show below that it has a coarse moduli space $Y_0(N)$ given by $\Gamma_0(N)\backslash\mathfrak{h}_i$ via assigning to each coset $\Gamma_0(N)\tau$ the classical $\Gamma_0(N)$-structure $(\mathbf{C}/\Lambda_\tau, \langle 1/N\rangle)$. Due to the non-rigidity, it can be proved that there is *no* $\Gamma_0(N)$-structure over $Y_0(N)$ inducing the bijection to the set of classical structures on the fibers; thus, there is no "fine moduli space".

The coarse moduli property ensures (via Example 5.3) that the natural transformation

$$w_N : (E \to M, C) \mapsto (E/C \to M, E[N]/C)$$

on sets of isomorphism classes of $\Gamma_0(N)$-structures, which is easily seen to be an involution (via $E/E[N] \simeq E$), arises from an involutive *holomorphic* automorphism of $Y_0(N)$. Concretely, via $Y_0(N)$ as the set of isomorphism classes of classical $\Gamma_0(N)$-structures, the substance is that the operation w_N on classical structures is really holomorphic as a map $Y_0(N) \to Y_0(N)$. *It is not necessary to compute explicit analytic formulas to justify this holomorphicity* (although finding such formulas may be psychologically reassuring); the coarse moduli space property alone guarantees holomorphicity by pure thought.

Likewise, once again using Example 5.3, for $N' \geq 1$ relatively prime to N, the maps $Y_0(NN') \rightrightarrows Y_0(N)$ defined by the natural transformations

$$(E \to M, C \times C') \mapsto (E \to M, C), \quad (E \to M, C \times C') \mapsto (E/C, C' \bmod C)$$

are both *holomorphic*. Note that this procedure requires that we can make sense of the desired operations in the *relative* setting over any complex manifold M (so we get a natural transformation T as in Example 5.3), even though in the end we can do computations with classical structures alone.

The main result on coarse moduli spaces is:

Theorem 5.5. *For a subgroup* $\Gamma \subset \mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$*, a coarse moduli space* Y_Γ *exists and has pure dimension 1. If* $N' \geq 3$ *is a multiple of* N *and* Γ' *is the preimage of* Γ *under* $\mathrm{GL}_2(\mathbf{Z}/N'\mathbf{Z}) \twoheadrightarrow \mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$ *then* $Y_\Gamma = Y_{\Gamma'} = \Gamma'\backslash Y(N')$ *with the orbit* $\Gamma' y \in \Gamma'\backslash Y_\zeta(N)$ *corresponding to the* Γ'*-structure induced by the full level-*N' *structure*

$$(E_{\zeta,y}, (P_\zeta(y), Q_\zeta(y))).$$

In particular, $\pi_0(Y_\Gamma)$ *is a principal homogeneous space for* $(\mathbf{Z}/N'\mathbf{Z})^\times/\det(\Gamma') = (\mathbf{Z}/N\mathbf{Z})^\times/\det(\Gamma)$*, so* Y_Γ *is connected if and only if* $\det : \Gamma \to (\mathbf{Z}/N\mathbf{Z})^\times$ *is surjective.*

In this theorem, the quotient $\Gamma'\backslash Y(N')$ as a Riemann surface is defined via §3.

Proof. It is harmless to replace (Γ, N) with (Γ', N'), so we may and do assume $N \geq 3$. Hence, $Y(N)$ exists. Any classical Γ-structure (E, α) can be enhanced to a full level-N structure (E, ϕ) with ϕ unique up to the Γ-action. Thus, the point $y \in Y(N)$ corresponding to (E, ϕ) is unique up to the Γ-action on $Y(N)$, so we get a bijection between $\Gamma\backslash Y(N)$ and the set of isomorphism classes of Γ-structures on classical elliptic curves (given by the recipe in the statement of the theorem).

By Proposition 5.2, our problem is to prove that for any elliptic curve $E \to M$ equipped with a Γ-structure α, the map of sets $M \to \Gamma\backslash Y(N)$ defined by carrying m to the isomorphism class of (E_m, α_m) is holomorphic. This problem is visibly local on M, so by shrinking M we can arrange that α is induced by a full level-N structure ϕ on $E \to M$. The pair (E, ϕ) is classified by a holomorphic map $M \to Y(N)$ to the moduli space for full level-N structures, and this holomorphic map carries m to the point classifying the classical pair (E_m, ϕ_m). Composing with the holomorphic quotient map $Y(N) \to \Gamma\backslash Y(N)$ then yields a holomorphic map $M \to \Gamma\backslash Y(N)$ which is as desired on underlying sets. ■

Example 5.6. We claim that the coarse moduli space $Y(1)$ for the functor F of isomorphism classes of elliptic curves is the complex plane, by assigning to any elliptic curve $E \to M$ the holomorphic map $j_{E/M} : M \to \mathbf{C}$. (Recall that $j_{E/M}$ really is holomorphic, due to the existence of Weierstrass models locally on M.) By the classical theory, $F(*) \to \mathbf{C}$ is bijective. Thus, by Proposition 5.2 the coarse moduli space property is precisely the known fact that $j_{E/M} : M \to \mathbf{C}$ is holomorphic for any $E \to M$.

It is clear by transitivity of quotients that $\mathrm{SL}_2(\mathbf{Z})\backslash\mathfrak{h}_i \to \mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})\backslash Y(N)$ is a holomorphic isomorphism for any $N \geq 3$, so the proof of Theorem 5.5 implies that the j-invariant of the Weiestrass family $\mathscr{E}^{(i)} \to \mathfrak{h}_i$

(which is the classical j-function!) must induce a holomorphic isomorphism $\mathrm{SL}_2(\mathbf{Z})\backslash\mathfrak{h}_i \to \mathbf{C}$. Of course, this fact is very well-known in the classical theory.

Consider $\Gamma \subset \mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$ with $N \geq 1$. The natural forgetful map $\pi : Y_\Gamma \to Y(1)$ (which is simply the j-invariant pointwise under the "explicit" description of $Y(1)$ provided by Example 5.6) must be holomorphic, due to the coarse moduli space property of $Y(1)$. Since Y_Γ and $Y(1)$ are complex manifolds of pure dimension 1 and π clearly has discrete fibers (so it is a "branched covering"), it makes sense to consider the ramification degree of π at a point $y \in Y_\Gamma$. We now explain how to interpret this ramification degree conceptually in terms of Γ-structures without reference to explicit half-plane quotients. Later this will enable us to compute the genus of a compactification X_Γ of a connected Y_Γ by purely moduli-theoretic means, without reference to $\mathfrak{h}_i^* := \mathfrak{h}_i \cup \mathbf{P}^1(\mathbf{Q})$ or its action by $\mathrm{SL}_2(\mathbf{Z})$. Also, the methods we use will carry over essentially verbatim to handle related problems in characteristic $p > 0$, especially the mysteries of ramification related to the "extra automorphisms" on supersingular elliptic curves in characteristics 2 and 3.

Proposition 5.7. *If (E, α) is the classical Γ-structure classified by $y \in Y_\Gamma$, then the ramification degree of $\pi : Y_\Gamma \to Y(1)$ at y is the size of the coset space $\mathrm{Aut}(E)/(\langle -1\rangle \cdot \mathrm{Aut}(E, \alpha))$.*

If $\det(\Gamma) = (\mathbf{Z}/N\mathbf{Z})^\times$ then the canonical Galois covering $\mathfrak{h}_i \to Y_\Gamma$ has ramification degree over y equal to the size of

$$\langle -1\rangle \cdot \mathrm{Aut}(E, \alpha)/\langle -1\rangle = \mathrm{Aut}(E, \alpha)/(\langle -1\rangle \cap \mathrm{Aut}(E, \alpha)).$$

We recall that in the classical theory, the elliptic curve $v^2 = u^3 - u$ with $j = 1728$ has automorphism group μ_4 of order 4, the elliptic curve $v^2 = u^3 - 1$ with $j = 0$ has automorphism group μ_6 of order 6, and all other elliptic curves have automorphism group μ_2 of order 2.

Proof. We may and do replace N with a multiple so that $N \geq 3$. By multiplicativity of ramification degrees and consideration of the "Galois" branched covering map $q : Y(N) \to \Gamma\backslash Y(N) = Y_\Gamma$, we are reduced to proving that for *any* Γ (such as $\Gamma = \mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$, which recovers $Y(1)$) and point $y \in Y_\Gamma$ corresponding to a pair (E, α), the common ramification degree of q at all points over y is equal to the size of $(\langle -1\rangle \cdot \mathrm{Aut}(E, \alpha))/\langle -1\rangle$ (which is $\mathrm{Aut}(E)/\langle -1\rangle$ when $\Gamma = \mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$).

The construction of the analytic structure on the quotient $Y_\Gamma = \Gamma\backslash Y(N)$ of the Riemann surface $Y(N)$ by the discontinuous action of Γ in the proof of Proposition 3.1 implies that the ramification degree of $Y(N) \to Y_\Gamma$ at a point $\widetilde{y}$ over $y \in Y_\Gamma$ coincides with the size of the quotient through which the stabilizer $\Gamma_{\widetilde{y}}$ acts faithfully on a small $\Gamma_{\widetilde{y}}$-stable connected open set around $\widetilde{y}$. Let (E, ϕ) be the full level-N structure corresponding to $\widetilde{y}$, so $\Gamma_{\widetilde{y}}$ is the group of elements $\gamma \in \Gamma$ such that $(E, \phi \circ \gamma^t) \simeq (E, \phi)$. Such an isomorphism is unique if it exists (since $N \geq 3$), and the underlying automorphism of E completely determines what γ is (since $\phi : (\mathbf{Z}/N\mathbf{Z})^2 \simeq E[N]$ is an isomorphism). Thus, we are precisely counting the size of the group of automorphisms of E whose effect on the set of Γ-structures on E preserves the class α arising from ϕ, and this is the group $\mathrm{Aut}(E, \alpha)$.

We conclude that $e(\widetilde{y}|y)$ is the size of the quotient of $\mathrm{Aut}(E, \alpha) \subset \Gamma$ that acts faithfully on a small connected open set around $\widetilde{y}$. We just have to prove that the kernel of this action is precisely $\langle -1\rangle \cap \mathrm{Aut}(E, \alpha)$, where this intersection is taken inside of $\mathrm{Aut}(E)$. Note that the element $-1 \in \mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$ acts trivially on the base $Y(N)$ of the universal full level-N structure since its effect on any full level-N structure $(\mathcal{E} \to M, \phi)$ is $(\mathcal{E} \to M, -\phi)$, which is isomorphic to $(\mathcal{E} \to M, \phi)$ via inversion on $\mathcal{E}$. (Beware that the effect of $-1 \in \mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$ on the universal elliptic curve over $Y(N)$ is nontrivial: it is inversion!) It therefore remains to prove that the only nontrivial element $\gamma \in \mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$ that acts trivially on a small connected open set in $Y(N)$ is -1. By analytic continuation, such a γ must preserve an entire connected component $Y_\zeta(N)$ of $Y(N)$ and in particular satisfy $\det\gamma = 1$, so $\gamma \in \mathrm{SL}_2(\mathbf{Z}/N\mathbf{Z})$. The given condition is that $(E \to M, \phi) \simeq (E \to M, \phi \circ \gamma^t)$ for every full level-N structure with Weil pairing ζ. But the locus of points on $Y_\zeta(N)$ with $j \in \{0, 1728\}$ is finite, as a given elliptic curve admits only *finitely many* full level-N structures, so there exists $y \in Y_\zeta(N)$ such that $j(y) \neq 0, 1728$ and hence the corresponding elliptic curve E_y has automorphism group $\langle -1\rangle$. Now pick any full level-N structure ϕ on E_y with Weil pairing ζ (as we may certainly do), so there is an isomorphism $(E_y, \phi) \simeq (E_y, \phi \circ \gamma^t)$. The underlying automorphism of E_y is ± 1, so we conclude that $\phi \circ \gamma^t$ is equal to ϕ or $-\phi = \phi \circ [-1]$. But $N \geq 3$, so full level-N structures are rigid and hence $\gamma = \pm 1$ in $\mathrm{SL}_2(\mathbf{Z}/N\mathbf{Z})$. ∎

Corollary 5.8. *The points $y \in Y_\Gamma$ at which $Y_\Gamma \to Y(1)$ is ramified must satisfy $j(y) = 0, 1728$, and for such y we must have $e(y) = 2$ when $j(y) = 1728$, and $e(y) = 3$ when $j(y) = 0$. These are exactly the points $y = (E, \alpha) \in Y_\Gamma$ with these j-values such that $\langle -1 \rangle \cdot \mathrm{Aut}(E, \alpha) \neq \mathrm{Aut}(E)$. In particular, if inversion always preserves Γ-structures then such y are precisely the pairs (E, α) such that α is* not *$\mathrm{Aut}(E)$-stable.*

Note that inversion preserves all Γ-structures if and only if $-1 \in \Gamma$ inside of $\mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$.

Proof. By Proposition 5.7, if y corresponds to a pair (E, α) then the ramification degree over $Y(1)$ divides $(1/2)\#\mathrm{Aut}(E)$. This can only be nontrivial when $j(E) = 0$ or $j(E) = 1728$, when it is 3 and 2 respectively. These cases correspond to when $\langle -1 \rangle \cdot \mathrm{Aut}(E, \alpha)$ is *not* equal to $\mathrm{Aut}(E)$. ∎

Now consider Γ such that $\det(\Gamma) = (\mathbf{Z}/N\mathbf{Z})^\times$, so Y_Γ is connected and there is a canonical factorization

$$\mathfrak{h}_i \to Y_\Gamma \to Y(1)$$

in which the composite map is the "j-invariant". Since $\mathfrak{h}_i \to Y(N')$ has no ramification for any $N' \geq 3$ (such as such an N' that is a multiple of N), it follows that $\mathfrak{h}_i \to Y(1)$ is also ramified only at points with $j = 0, 1728$, and that at such points the ramification degree is 3 and 2 respectively. It follows that any any such points on $\mathfrak{h}_i$, the map $\mathfrak{h}_i \to Y_\Gamma$ is ramified if and only if $Y_\Gamma \to Y(1)$ is *not* ramified at the image in Y_Γ; classically these are called *elliptic points* on Y_Γ, and one distinguishes them according to whether the ramification under $\mathfrak{h}_i$ is 2 or 3. By Corollary 5.8, if inversion preseves all Γ-structures (i.e., $-1 \in \Gamma$) then the elliptic points on Y_Γ are precisely those (E, α) with $j(E) \in \{0, 1728\}$ for which α *is* $\mathrm{Aut}(E)$-stable. (Beware that if Γ is not normal in $\mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$ then $Y_\Gamma \to Y(1)$ typically fails to be a "generically" Galois covering, so elliptic and non-elliptic points can lie in a common fiber.)

6. Elliptic points

The results on moduli-theoretic interpretation of ramification degrees at the end of §5 make it possible to give conceptual proofs of results proved in the classical analytic theory of modular curves via elaborate group-theoretic calculations with $\mathrm{SL}_2(\mathbf{Z})$, such as counts of elliptic points. We offer two examples, and the interested reader can adapt the technique to other examples.

Example 6.1. Assume $-1 \in \Gamma$ and $\det(\Gamma) = (\mathbf{Z}/N\mathbf{Z})^\times$, so the elliptic points in $y \in Y_\Gamma$ with order-p ramification for $p = 3$ (resp. $p = 2$) are in natural bijection with the set of $\mathrm{Aut}(E)$-stable Γ-structures α on the classical elliptic curve E_0 with $j(E_0) = 0$ (resp. E_{1728}). Let's see how this works out the for example of cyclic subgroups of order N, corresponding to $\Gamma = \{(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix})\}$. We first consider $p = 3$.

Since $\mathrm{H}_1(E_0, \mathbf{Z})$ is a rank-2 finite free $\mathbf{Z}$-module with as faithful action of $\mathbf{Z}[\zeta_3]$, it must be an invertible $\mathbf{Z}[\zeta_3]$-module and thus free of rank 1 (as $\mathbf{Z}[\zeta_3]$ has trivial class group). Thus, $E_0[N]$ is a free $\mathbf{Z}[\zeta_3]/(N)$-module of rank 1 on which the $\mathrm{Aut}_0(E)$-action is exactly the scaling action by μ_6. Hence, $\mathrm{Aut}(E_0)$-stability amounts to being a $\mathbf{Z}[\zeta_3]$-submodule, which is to say an ideal. The count of ideals is a purely *local* problem: we can decompose N into rational prime powers and treat each of these separately.

For a prime p, how many $\mathbf{Z}/(p^r)$-module direct factors of $\mathbf{Z}[\zeta_3]/(p^r)$ are ideals? If p splits in $\mathbf{Z}[\zeta_3]$ (i.e., $(-3|p) = 1$) then there are exactly two such ideals, corresponding to the two local factors rings of $\mathbf{Z}[\zeta_3]/(p^r)$. Otherwise $\mathbf{Z}[\zeta_3]_{(p)}$ is already local and hence the collection of ideals in $\mathbf{Z}[\zeta_3]/(p^r)$ is *linearly ordered.* Hence, if there is such an ideal for some $r \geq 1$ then its reduction modulo p must be such an ideal in $\mathbf{Z}[\zeta_3]/(p)$, yet this is a *field* (and so has no nonzero proper ideals) when p is inert (i.e., $(-3|p) = -1$) and is $\mathbf{F}_3[\varepsilon]/(\varepsilon^2)$ when $p = 3$. Consequently, there are no such ideals for inert p and the only possibility for the ideal when $p = 3$ is the maximal ideal (by Nakayama's Lemma). By length considerations, the maximal ideal cannot work for $p = 3$ when $r > 1$ but it does work for $r = 1$.

Summarizing, the number of ideals in $\mathbf{Z}[\zeta_3]/(p^r)$ that are $\mathbf{Z}/(p^r)$-module direct factors is $1 + (-3|p)$ when $p \neq 3$ and is $1 = 1 + (-3|3)$ (by convention) when $p = 3$ with $r = 1$ but is 0 when $p = 3$ with $r > 1$. In terms of the original N, this count of ideals is 0 when $9|N$ and is $\prod_{p|N}(1 + (-3|p))$ otherwise. So voila, we have recovered the classical count of order-3 elliptic points on $Y_0(N)$! The case of order-2 elliptic points goes exactly the same way, using $\mathbf{Z}[i]$ in place of $\mathbf{Z}[\zeta_3]$ and $p=2$ in place of $p=3$ and "$4|N$" in place of "$9|N$".

Example 6.2. We now consider a generalization of Exercise 4(iv) in HW4, replacing the prime there with a general "level". For any integer $N \geq 1$, a *Cartan subgroup* of $\mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$ is the group of units of a rank-2 finite étale $\mathbf{Z}/N\mathbf{Z}$-algebra A (relative to a choice of $\mathbf{Z}/N\mathbf{Z}$-basis of A, the choice of which has the effect of conjugation in $\mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$). There is a ring decomposition $A = \prod_{p|N} A_p$, where each A_p is a rank-2 finite étale $\mathbf{Z}/(p^{r_p})$-algebra, with $r_p = \mathrm{ord}_p(N)$. Since étale algebras are uniquely determined by their quotient modulo nilpotents in the base, there are only two possibilities for A_p up to isomorphism since $\mathbf{F}_p$ has only two rank-2 étale algebras, namely $\mathbf{F}_p \times \mathbf{F}_p$ and $\mathbf{F}_{p^2}$. Concretely, the corresponding possibilities for A_p are $(\mathbf{Z}/(p^{r_p}))^2$ and $W(\mathbf{F}_{p^2})/(p^{r_p})$ (called the *split* and *non-split* cases respectively). There is also a unique nontrivial $\mathbf{Z}/(p^{r_p})$-algebra automorphism of A_p, denoted $a \mapsto \overline{a}$. (This is the swap of factors in the split case, and the action of the nontrivial element of $\mathrm{Gal}(\mathbf{F}_{p^2}/\mathbf{F}_p)$ in the non-split case.)

Compatibly with the decomposition $\mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z}) \simeq \prod_{p|N} \mathrm{GL}_2(\mathbf{Z}/(p^{r_p}))$ we have

$$A^\times = \prod_{p|N} A_p^\times.$$

Thus, the normalizer Γ_A of $A^\times$ in $\mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$ decomposes as the analogous direct product of the normalizer of A_p in $\mathrm{GL}_2(\mathbf{Z}/(p^{r_p}))$ for $p|N$. Since A_p is its own centralizer in $\mathrm{Mat}_2(\mathbf{Z}/(p^{r_p}))$ (as a free A_p-module of rank 1 has A_p-linear endomorphism ring equal to A_p) and $A_p^\times$ generates A_p as a $\mathbf{Z}/(p^{r_p})$-algebra (as we may check modulo p by Nakayama's Lemma, where it can be seen for both $\mathbf{F}_p \times \mathbf{F}_p$ and $\mathbf{F}_{p^2}$ by inspection), it follows that the normalizer Γ_{A_p} is an index-2 extension of $A_p^\times$ whose nontrivial coset acts on $A_p^\times$ through $a_p \mapsto \overline{a}_p$.

Arguing exactly as in Exercise 4(iv) of HW4, for the subgroup Γ_A in $\mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$ (which is well-defined up to conjugation) we see that Y_{Γ_A} is the coarse moduli space for elliptic curves E equipped with a structure of invertible A-module on $E[N]$ taken up to the action of the group $\mathrm{Aut}(A) = (\mathbf{Z}/2\mathbf{Z})^{\omega(N)}$ (where $\omega(N)$ is the number of distinct prime factors of N). Since $-1 \in \Gamma_A$ and $\det(\Gamma_A) = (\mathbf{Z}/N\mathbf{Z})^\times$, we can count the elliptic points on Y_Γ with order 2 and order 3 by using the same style of procedure as above. In particular, the counting problem again decomposes into a product of local contributions according to the decomposition of $\mathbf{Z}/N\mathbf{Z}$ into the product of rings $\mathbf{Z}/(p^{r_p})$ for $p|N$. Hence, the essential case is $N = p^r$, so we now consider such N. We will work out the case of order-2 elliptic points, as the answer in this case is more complicated.

Consider the elliptic curve E with $j(E) = 1728$, so $\mathrm{End}(E) = \mathbf{Z}[i]$ and $E[p^r]$ is a free $\mathbf{Z}[i]/(p^r)$-module of rank 1. We seek to count the number of invertible A-module structures on $E[p^r]$ which are invariant up to $\mathrm{Aut}(A)$ when composed with conjugation by a generator of μ_4, and consider such structures up to composing with $\mathrm{Aut}(A)$. That is, we demand that the A-linear structure either is $\mathbf{Z}[i]$-linear or commutes with the $\mathbf{Z}[i]$-structure up to $a \mapsto \overline{a}$, and we count the number of such structures up to $\mathrm{Aut}(A)$. Note also that the invertibility of the A-module structure amounts to the faithfulness of the A-linear action on $E[p^r]$.

First consider the contribution from the $\mathbf{Z}[i]$-linear structures. Since $E[p^r]$ is a free $\mathbf{Z}[i]/(p^r)$-module of rank 1, the $\mathbf{Z}[i]$-linear case corresponds to injective ring homomorphisms $A \to \mathbf{Z}[i]/(p^r)$ taken up to composition with $\mathrm{Aut}(A)$. Such injective maps must be isomorphisms (as source and target have the same size), so any two such maps are related via $\mathrm{Aut}(A)$. In other words, the contribution from the $\mathbf{Z}[i]$-linear A-structures amounts to determining whether or not A is abstractly isomorphic to $\mathbf{Z}[i]/(p^r)$, in which case the contribution to the total count of interest is 1, and otherwise the contribution is 0. So this part is now clear, since A is finite étale over $\mathbf{Z}/(p^r)$ with rank 2: there is no contribution when $p=2$, and for odd p (so $\mathbf{Z}[i]/(p^r)$ is a rank-2 finite étale $\mathbf{Z}/(p^r)$-algebra) we get a contribution of 1 precisely when $A \simeq \mathbf{Z}[i]/(p^r)$ (i.e., for split A if and only if $p \equiv 1 \bmod 4$, and for non-split A if and only if $p \equiv 3 \bmod 4$).

The remaining contribution is when i-conjugation normalizes the A-structure via the nontrivial automorphism $a \mapsto \overline{a}$. These come in pairs related through the action of the nontrivial automorphism of A, so the count of interest is half the number of such A-structures. The result depends on whether A is split or non-split. We will work out the non-split case, and leave it to the interested reader to work out the split case. To maintain a conceptual approach, we will use some facts from the theory of associative algebras over artin local rings (such as $\mathbf{Z}/(p^r)$), generalizing classical facts from the theory of central simple algebras over fields (such as $\mathbf{F}_p$). Two useful references are §1 in Chapter IV of Milne's book "Étale cohomology", and part I of Grothendieck's sequence of three papers "Le groupe de Brauer".

Now $A = W(\mathbf{F}_{p^2})/(p^r)$. Consider the following quaternion-type construction: $D = A \oplus Ai$ as an A-module, with algebra structure given by $iai^{-1} = \overline{a}$ and $i^2 = -1$. This is a rank-4 finite flat associative $\mathbf{Z}/(p^r)$-algebra that is finite free of rank 2 over both A and $\mathbf{Z}[i]/(p^r)$, and we are seeking to count the number of $\mathbf{Z}[i]/(p^r)$-algebra homomorphisms

$$D \to \mathrm{End}_{\mathbf{Z}/(p^r)}(E[p^r]) \simeq \mathrm{End}_{\mathbf{Z}/(p^r)}(\mathbf{Z}[i]/(p^r)) \simeq \mathrm{Mat}_2(\mathbf{Z}/(p^r))$$

that are injective on A. In fact, the injectivity on A is automatic because any such algebra homomorphism *must* be an isomorphism. Indeed, it suffices to check this modulo p, and I claim that the 4-dimensional associative $\mathbf{F}_p$-algebra $D/(p)$ is a matrix algebra (and thus is a simple ring). In fact, since $A/(p) = \mathbf{F}_{p^2}$ (as we are in the non-split case), by construction $D/(p)$ is the cyclic algebra $(\mathbf{F}_{p^2}/\mathbf{F}_p, -1)$ in the sense of Dickson, and cyclic algebras are always central simple. But by Wedderburn's theorem, over a finite field all central simple algebras are matrix algebras, so indeed $D/(p) \simeq \mathrm{Mat}_2(\mathbf{F}_p)$ for dimension reasons.

We can do even better: D is necessarily a matrix algebra over $\mathbf{Z}/(p^r)$! Indeed, since D is an associative algebra over the local ring $\mathbf{Z}/(p^r)$ and is finite free as a module, with special fiber $D/(p)$ over $\mathbf{F}_p$ that is a central simple algebra, by definition D is an *Azumaya algebra* (see Theorem 5.1 and Corollary 5.2 in part I of Grothendieck's papers on the Brauer group, or §1 in Chapter IV of Milne's book "Étale Cohomology"). By basic deformation-theoretic facts in the theory of Azumaya algebras over artin local rings (see §4, especially Corollary 4.2, in Grothendieck's paper, or Proposition 1.6 in Chapter IV of Milne's book), D must be a matrix algebra because its special fiber is a matrix algebra. Thus, there does exist an isomorphism $D \simeq \mathrm{End}_{\mathbf{Z}/(p^r)}(E[p^r])$ as $\mathbf{Z}/(p^r)$-algebras since both sides are isomorphic to $\mathrm{Mat}_2(\mathbf{Z}/(p^r))$. Such an isomorphism can even be found that is $\mathbf{Z}[i]/(p^r)$-linear provided that all $\mathbf{Z}/(p^r)$-algebra embeddings $\mathbf{Z}[i]/(p^r) \hookrightarrow \mathrm{Mat}_2(\mathbf{Z}/(p^r))$ are related to each other via conjugation. (This is a variant of Skolem–Noetherian over the artin ring $\mathbf{Z}/(p^r)$.) Any two such embeddings correspond to invertible $\mathbf{Z}[i]/(p^r)$-module structures on the $\mathbf{Z}/(p^r)$-module $(\mathbf{Z}/(p^r))^{\oplus 2}$, and the conjugacy amounts to the evident fact that such module structures are abstractly $\mathbf{Z}[i]/(p^r)$-linearly isomorphic (because $\mathbf{Z}[i]/(p^r)$ is a semi-local ring).

Thus, there always exists *at least one* $\mathbf{Z}[i]/(p^r)$-algebra isomorphism $D \simeq \mathrm{End}_{\mathbf{Z}/(p^r)}(E[p^r])$, and so any two are off from each other by a $\mathbf{Z}[i]/(p^r)$-algebra automorphism of $\mathrm{End}_{\mathbf{Z}/(p^r)}(E[p^r])$. But in this matrix algebra over $\mathbf{Z}/(p^r)$ the canonically embedded subalgebra $\mathbf{Z}[i]/(p^r)$ is its own centralizer (since any invertible module over a ring, such as $\mathbf{Z}[i]/(p^r)$, have precisely scalar endomorphisms), so from one $\mathbf{Z}[i]/(p^r)$-algebra isomorphisms we get all others by conjugation against $(\mathbf{Z}[i]/(p^r))^\times$. This conjugation only matters modulo the overlap $(\mathbf{Z}/(p^r))^\times$ with the center, so the number of such isomorphisms is the size of $(\mathbf{Z}[i]/(p^r))^\times/(\mathbf{Z}/(p^r))^\times$. This is $(p+1)p^{r-1}$ for p inert in $\mathbf{Z}[i]$, $(p-1)p^{r-1}$ for p split in $\mathbf{Z}[i]$, and 2^r for $p = 2$. Dividing by 2 (to account for the $\mathrm{Aut}(A)$-equivalence) and adding in the earlier count of $\mathbf{Z}[i]/(p^r)$-linear faithful A-module structures on $E[p^r]$ yields that when $N = p^r$, the number of order-2 elliptic points is $1 + p^{r-1}(p+1)/2$ for $p \equiv 3 \bmod 4$, $p^{r-1}(p-1)/2$ for $p \equiv 1 \bmod 4$, and 2^{r-1} for $p = 2$.