21.1 Level structure

Let $N \le \mathbb{Z}_{\ge 1}$ and let E/k be an elliptic curve over a perfect field k of characteristic prime to N. To simply notation, we put $\mathbb{Z}(N) := \mathbb{Z}/N\mathbb{Z}$ and $\mathrm{GL}_2(N) := \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$.

Each basis (P_1, P_2) for $E[m] = \langle P_1, P_2\rangle$ defines an isomorphism $\iota\colon E[N] \xrightarrow{\sim} \mathbb{Z}(N)^2$ that sends P_1 to $e_1 := \left(\begin{smallmatrix}1\\0\end{smallmatrix}\right)$ and P_2 to $e_2 := \left(\begin{smallmatrix}0\\1\end{smallmatrix}\right)$. This induces an isomorphism $\mathrm{Aut}(E[N]) \xrightarrow{\sim} \mathrm{GL}_2(N)$ that we also denote ι. For $\phi \in \mathrm{Aut}(E[N])$ with

$$\begin{aligned}\phi(P_1) &= aP_1 + cP_2\\ \phi(P_2) &= bP_1 + dP_2\end{aligned}$$

we define

$$\iota(\phi) := \begin{pmatrix} a & b\\ c & d\end{pmatrix},$$

so that

$$\begin{aligned}\iota(\phi(P_1)) &= \left(\begin{smallmatrix}a\\c\end{smallmatrix}\right) = \left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right)\left(\begin{smallmatrix}1\\0\end{smallmatrix}\right) = \iota(\phi)\iota(P_1)\\ \iota(\phi(P_2)) &= \left(\begin{smallmatrix}b\\d\end{smallmatrix}\right) = \left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right)\left(\begin{smallmatrix}0\\1\end{smallmatrix}\right) = \iota(\phi)\iota(P_2).\end{aligned}$$

This is consistent with the **left action** of $\mathrm{GL}_2(N)$ on $\mathbb{Z}(N)^2$. The isomorphism ι allows us to view the mod-N Galois representation

$$\rho_{E,N}\colon \mathrm{Gal}_k \to \mathrm{Aut}(E[N]) \xrightarrow[\sim]{\iota} \mathrm{GL}_2(N)$$

as a continuous group homomorphism $\mathrm{Gal}_k \to \mathrm{GL}_2(N)$.

When k has characteristic zero, each compatible system of bases for $E[N]$ for all positive integers N induces an isomorphism $\iota\colon \mathrm{Aut}(T(E)) \xrightarrow{\sim} \mathrm{GL}_2(\widehat{\mathbb{Z}})$, where

$$T(E) := E(\bar{k})_{\mathrm{tor}} = \varprojlim_N E[N] \simeq \widehat{\mathbb{Z}}^2$$

is the adelic Tate module. The isomorphism ι allows us to view the Galois representation

$$\rho_E\colon \mathrm{Gal}_k \to \mathrm{Aut}(T(E)) \xrightarrow[\sim]{\iota} \mathrm{GL}_2(\widehat{\mathbb{Z}})$$

as a continuous group homomorphism $\mathrm{Gal}_k \to \mathrm{GL}_2(\widehat{\mathbb{Z}})$. Recall that the level of an open subgroup $H \le \mathrm{GL}_2(\widehat{\mathbb{Z}})$ is the least $N \in \mathbb{Z}_{\ge 1}$ for which $H = \pi_N^{-1}(\pi_N(H))$, where $\pi_N\colon \mathrm{GL}_2(\widehat{\mathbb{Z}}) \to \mathrm{GL}_2(N)$ is the canonical projection associated to the inverse limit $\mathrm{GL}_2(\widehat{\mathbb{Z}}) \simeq \varprojlim_N \mathrm{GL}_2(N)$.

Definition 21.1. For $H \le \mathrm{GL}_2(N)$, an H-level structure on an elliptic curve E is an equivalence class $[\iota]_H$ of isomorphisms $\iota\colon E[N] \to \mathbb{Z}(N)^2$, where $\iota \sim \iota'$ whenever $\iota = h \circ \iota'$ for some $h \in H$, where $h \in \mathbf{H} \le \mathrm{GL}_2(N) = \mathrm{Aut}(E[N])$ acts as an automorphism of $\mathbb{Z}(N)^2$; this action gives the abelian group $\mathrm{Hom}(E[N], \mathbb{Z}(N)^2)$ the structure of a left H-module, and we can equivalently view $[\iota]_H = \{h \circ \iota : h \in H\}$ as the H-orbit of an isomorphism $\iota \in \mathrm{Hom}(E[N], \mathbb{Z}(N)^2)$.

For open $H \le \mathrm{GL}_2(\widehat{\mathbb{Z}})$ of level N, an H-level structure on E is a $\pi_N(H)$-level structure on E; equivalently, an H-level structure on E is the H-orbit of an isomorphism $\iota \in \mathrm{Hom}(T(E), \widehat{\mathbb{Z}}^2)$.

When $H \in \mathrm{GL}_2(N)$ is trivial, the H-orbits of isomorphisms $\iota \in \mathrm{Hom}(E[N], \mathbb{Z}(N)^2)$ are singletons, each corresponding to a choice of basis (P_1, P_2) for $E[N]$. This is the full level-N structure on E. As noted in the previous lecture, the non-cuspidal points on the modular curve

$X(N) := \Gamma(N)\backslash\mathbf{H}^*$ correspond to isomorphism classes of triples (E, P_1, P_2), equivalently, elliptic curves E equipped with full level-N structure. Each $H \le \mathrm{GL}_2(N)$ acts on $X(N)$ via automorphisms, and non-cuspidal points on the quotient $H\backslash X(N)$ correspond to isomorphism classes of elliptic curves with an H-level structure.

Alternatively, we can formally define the modular curve X_H as the coarse moduli space associated to the stack $\mathscr{M}_H$ over $\operatorname{Spec}\mathbb{Z}[1/N]$ whose non-cuspidal points parameterize elliptic curves with H-level structure, as defined by Deligne and Rapoport [1]. The theory of stacks is beyond the scope of this course, but we can describe this stack very explicitly by giving its functor of points, and this description allows us to compute many invariants of X_H that can be difficult to compute using a quotient of $X(N)$, especially when N is large.

As a stack over $\mathbb{Z}[1/N]$ the modular curve X_H can always be viewed as a smooth projective curve over $\mathbb{Q}$ that has good reduction at all primes $p \nmid N$; this amounts to taking the base change to $\mathbb{Q}$ and forgetting its moduli structure. But X_H is a nice curve (smooth, projective, geometrically integral) only when $\det(H) = \widehat{\mathbb{Z}}^\times$, so we will restrict our attention to this case, which is the relevant case to consider if one is interested in elliptic curves over $\mathbb{Q}$.

If we put $\Gamma_H := \pm H \cap \mathrm{SL}_2(\mathbb{Z})$, then over the cyclotomic field $\mathbb{Q}(\zeta_N)$, every component of the base change of the curve X_H is isomorphic to the (nice) algebraic curve corresponding to the Riemann surface $X_{\Gamma_H} := \Gamma_H\backslash\mathbf{H}^*$, which *a priori* is defined over $\mathbb{C}$ but admits a model over $\mathbb{Q}(\zeta_N)$ (but not necessarily over $\mathbb{Q}$, which is another reason to consider X_H).

The group $\Gamma_H \le \mathrm{SL}_2(\mathbb{Z})$ is necessarily a congruence subgroup, since it contains $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$, but it may also contain $\mathrm{SL}_2(\mathbb{Z}/M\mathbb{Z})$ for some proper divisor M of N. Thus the level of the congruence subgroup Γ_H need not coincide with the level of H, although it will necessarily divide it. Indeed, there will typically be infinitely many non-conjugate open subgroups $H \le \mathrm{GL}_2(\widehat{\mathbb{Z}})$ of varying level N that share the same intersection Γ_H with $\mathrm{SL}_2(\mathbb{Z})$. The corresponding modular curves X_H are all isomorphic over $\mathbb{Q}^{\mathrm{cyc}} = \bigcup_N \mathbb{Q}(\zeta_N)$, but not over $\mathbb{Q}$; they are twists of X_{Γ_H}.

21.2 Twists

Definition 21.2. Two curves X, X' over a field k are twists (of each other) if $X_L \simeq X'_L$ for some extension L/k. The same definition also applies to abelian varieties (and more generally to any category of objects over a field k that has an appropriate notion of base change).

For a fixed curve X/k, the k-isomorphism classes of twists X' of X are parameterized by the cohomology set $H^1(\mathrm{Gal}_k, \mathrm{Aut}(X_{\bar{k}}))$. Note that $\mathrm{Aut}(X_{\bar{k}})$ need not be abelian, so this is a pointed set and not necessarily a group. Twisting is a subtle topic in general, but it is quite simple when $\mathrm{Aut}(X_{\bar{k}})$ is a finite abelian group on which Gal_k acts trivially, which is true in almost all cases where X is an elliptic curve.

For an elliptic curve E/k with $j(E) \ne 0, 1728$ the only non-trivial isomorphism of $E_{\bar{k}}$ is the map that sends P to $-P$, in which case $\mathrm{Aut}(E_{\bar{k}}) = \mathrm{Aut}(E) \simeq \{\pm 1\}$ is a cyclic group of order 2 with trivial Gal_k-action. In this situation $H^1(\mathrm{Gal}_k, \mathrm{Aut}(E_{\bar{k}}))$ consists of all continuous homomorphisms $\mathrm{Gal}_k \to \{\pm 1\}$, each of which is either trivial (corresponding to a trivial twist $E' \simeq E$) or has a kernel whose fixed field is a quadratic extension L/k over which $E'_L \simeq E_L$ for some $E' \not\simeq E$ that is unique up to k-isomorphism; this is the quadratic twist of E by L/k.

When k does not have characteristic 2 or 3, we can assume E is defined by a Weierstrass equation $y^2 = x^3 + Ax + B$, in which case the map $P \mapsto -P$ simply negates the y-coordinate of P, and if we write the fixed field of the kernel of a non-trivial element of $H^1(\mathrm{Gal}_k, \mathrm{Aut}(E_{\bar{k}}))$ as $L = k(\sqrt{d})$ for some non-square $d \in k$, the twist E' of E by L is isomorphic to $dy^2 = x^3 + Ax + B$ (and also to $y^2 = x^3 + d^2Ax + d^3B$).

Even if $j(E) = 0, 1728$, provided k does not have characteristic 2 or 3 the automorphism group $\mathrm{Aut}(E_{\bar{k}})$ is a cyclic of order 4 or 6 (for $j(E) = 1728$ and $j(E) = 0$, respectively). In this situation $\mathrm{Aut}(E_{\bar{k}})$ may not be a trivial Gal_k-module (this depends on whether k contains a primitive 4th or 6th root of unity), but in any case it is still easy to understand the Gal_k-module structure of $\mathrm{Aut}(E_{\bar{k}})$ and write down Weierstrass equations for twists of E.

21.3 Modular curves X_H

Let us now describe X_H in terms of its functor of points. As with quotients of the upper half plane, we will first describe Y_H, which effectively solves the moduli problem, and then explain how to add “cusps" to Y_H so that X_H can be viewed as a smooth projective curve.

Let H be an open subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ of level N with $\det(H) = \widehat{\mathbb{Z}}^\times$ and let k be a perfect field of characteristic prime to N. The set $Y_H(\bar{k})$ consists of equivalence classes of pairs $(E, [\iota]_H)$, where $E/\bar{k}$ is an elliptic curve and $[\iota]_H$ is an H-level structure on E. We have an equivalence $(E, [\iota]_H) \sim (E', [\iota']_H)$ whenever there is an isomorphism $\phi\colon E \to E'$ for which the induced isomorphism $\phi_N\colon E[N] \to E'[N]$ satisfies $\iota \sim \iota' \circ \phi_N$, meaning $\iota = h \circ \iota' \circ \phi_N$ for some $h \in \pi_N(H)$.

Equivalently, $Y_H(\bar{k})$ consists of pairs $(j(E), \alpha)$, where $\alpha = HgA_E$ is a double coset in

$$H\backslash \mathrm{GL}_2(N)/A_E,$$

where $A_E \coloneqq \{\varphi_N : \varphi \in \mathrm{Aut}(E)\}$ with $\varphi_N \coloneqq \iota(\varphi_{|_{E[N]}})$. For $j(E) \neq 0, 1728$ we have $A_E = \{\pm 1\}$, and if $-1 \in H$ we can identify double cosets in $H\backslash \mathrm{GL}_2(N)/\{\pm 1\}$ with the right cosets in $H\backslash \mathrm{GL}_2(N)$.

Each $\sigma \in \mathrm{Gal}_k$ induces an isomorphism $E^\sigma[N] \to E[N]$ defined by $P \mapsto \sigma^{-1}(P)$, where E^σ is the elliptic curve obtained by letting σ act on the coefficients of an equation defining E; let σ^{-1} denote this isomorphism. We have a right Gal_k-action on $Y_H(\bar{k})$ given by

$$(E, [\iota]_H) \mapsto (E^\sigma, [\iota \circ \sigma^{-1}]_H),$$

and define $Y_H(k)$ to be the fixed points of this action. Each point in $Y_H(k)$ is represented by a pair $(E, [\iota]_H)$, where E/k is an elliptic curve and for every $\sigma \in \mathrm{Gal}_k$ there is a $\varphi \in \mathrm{Aut}(E_{\bar{k}})$ and $h \in H$ such that

$$\iota \circ \sigma^{-1} = h \circ \iota \circ \varphi_N.$$

Equivalently, $Y_H(k)$ consists of pairs $(j(E), \alpha)$ where $j(E) \in k$ is the j-invariant of an elliptic curve E/k and $\alpha = HgA_E \in H$ is a double coset with $Hg\rho_{E,N}(\sigma)A_E = HgA_E$ for every $\sigma \in \mathrm{Gal}_k$.

For E/k with $j(E) \neq 0, 1728$, if $-1 \in H$ we can determine the k-rational points on Y_H corresponding to E (if any) by computing the fixed points of $\rho_{E,N}(\mathrm{Gal}_k) \subseteq \mathrm{GL}_2(N)$ in the permutation representation of $\mathrm{GL}_2(N)$ given by the right action of $\mathrm{GL}_2(N)$ on $H\backslash \mathrm{GL}_2(N)$. This amounts to computing the rational points in the fiber of $X_H \to X(1)$ above the point $j(E)$ on $X(1) \simeq \mathbb{P}^1_k$.

Proposition 21.3. *Let H be an open subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ of level N and E/k be an elliptic curve. If $\rho_{E,N}(\mathrm{Gal}_K) \leq H$ then there exists an isomorphism $\iota\colon E[N] \xrightarrow{\sim} \mathbb{Z}(N)^2$ for which $(E, [\iota]_H) \in Y_H(k)$.*

Conversely, if $(E, [\iota]_H) \in Y_H(k)$, then for every twist E' of E there exists $\iota'\colon E'[N] \xrightarrow{\sim} \mathbb{Z}(N)^2$ with $(E', [\iota']_H) \in Y_H(k)$, and if $\mathrm{Aut}(E_{\bar{k}}) = \{\pm 1\}$ for at least one twist E' we have $\rho_{E',N}(\mathrm{Gal}_k) \leq H$.

Proof. If $\rho_{E,N}(\mathrm{Gal}_k) \leq H$ then Gal_k fixes the trivial double coset $H\alpha A_E$ with $\alpha = 1$, and we have $(j(E), \alpha) \in Y_H(k)$. For the converse, if E' is a twist of E, then we have an isomorphism $\phi\colon E'_{\bar{k}} \xrightarrow{\sim} E_{\bar{k}}$ that induces an isomorphism $\phi_N\colon E'[N] \xrightarrow{\sim} E[N]$, and if we put $\iota' = \iota \circ \phi_N$ the pairs $(E, [\iota]_H)$ and $(E', [\iota']_H)$ are equivalent (as witnessed by ϕ) and represent the same point in $Y_H(\bar{k})$, so if $(E, [\iota]_H)$ lies in $Y_H(k)$ then so does $(E', [\iota']_H)$. See Problem 2 on Problem Set 7 for the final claim. $\square$

Remark 21.4. The final claim of Proposition 21.3 actually holds whenever $\mathrm{Aut}(E_{\bar{k}})$ is cyclic, which is always true provided k does not have characteristic 2 or 3; see [2, Proposition 12.2.1].

The modular curve X_H is obtained from Y_H by adjoining cusps X_H^∞, whose functor of points we now describe. The cusps in $X_H^\infty(\bar{k})$ correspond to double cosets $H\backslash\mathrm{GL}_2(N)/U(N)$, where $U(N) = \langle \pm \left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)\rangle$ corresponds to the stabilizer of ∞ in $\mathrm{SL}_2(\mathbb{Z})$. We equip $X_H^\infty(\bar{k})$ with a right Gal_k-action $hgu \mapsto hg\chi_N(\sigma)u$, where the cyclotomic character $\chi_N(\sigma) := \left(\begin{smallmatrix}e&0\\0&1\end{smallmatrix}\right)$ is defined by $\sigma(\zeta_N) = \zeta_N^e$. Rational cusps in $X_H^\infty(k)$ corresponds to double cosets in $H\backslash\mathrm{GL}_2(N)/U(N)$ that are fixed by $\chi_N(\mathrm{Gal}_k)$.

21.4 Computing the genus

The genus of a curve is invariant under base change. If follows that if we puts $\Gamma_H := \pm H \cap \mathrm{SL}_2(\mathbb{Z})$ then $g(X_H) = g(X_{\Gamma_H})$ (here we are assuming $\det(H) = \widehat{\mathbb{Z}}^\times$ so that X_H is geometrically connected, but otherwise we define the genus of H to be the genus of each of its geometric components, all of which are isomorphic to X_{Γ_H}). In fact the genus of X_{Γ_H} depends only on the intersection of Γ_H with $\mathrm{SL}_2(N)$, where N is any multiple of the level of Γ_H; we can take N to be the level of H, but it is more efficient to take N to be the level of Γ_H.

This allows us to compute the genus of X_H via the formula

$$g(H) = g(\Gamma_H) = 1 + \frac{i(\Gamma_H)}{12} - \frac{\nu_2(\Gamma_H)}{4} - \frac{\nu_3(\Gamma_H)}{3} - \frac{\nu_\infty(\Gamma_H)}{2},$$

where we view Γ_H as a subgroup of $\mathrm{SL}_2(N)$ that contains -1, let $i(\Gamma_H) := [\mathrm{SL}_2(N) : \Gamma_H]$, let $\nu_2(\Gamma_H)$ and $\nu_3(\Gamma_H)$ count right cosets in $\Gamma_H\backslash\mathrm{SL}_2(N)$ containing conjugates of $\left(\begin{smallmatrix}0&1\\-1&0\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}0&1\\-1&-1\end{smallmatrix}\right)$, respectively, and let $\nu_\infty(\Gamma_H)$ count the orbits of $\Gamma_H\backslash\mathrm{SL}_2(N)$ under the right action of $\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$.

References

[1] Pierre Deligne and Michael Rapoport, *Les schémas de modules de courbes elliptiques*, Modular functions of one variable, II (Proc. Internat. Summer School, Univ Antwerp, 1972), 1973, pp. 143–316, Lecture Notes in Mathematics **349**, Springer.

[2] Jeremy Rouse, Andrew V. Sutherland, and David Zureick-Brown, with an appendix by John Voight, *ℓ-adic images of Galois for elliptic curves over $\mathbb{Q}$*, Forum of Mathematics, Sigma **10** (2022), e62.

[3] Andrew V. Sutherland, *Lecture notes for Elliptic Curves (18.783)*, 2023.