Modular Curves

David Loeffler
Notes by Florian Bouyer

Contents

Why study modular curves?

1. They give more information on modular forms.
2. They give friendly examples of moduli spaces.

0 Waffle

Let $\mathcal{H} = \{z \in \mathbb{C} | \operatorname{im} z > 0\}$. We have that the group $\mathrm{SL}_2(\mathbb{R})$ acts on $\mathcal{H}$. Take $\Gamma < \mathrm{SL}_2(\mathbb{Z})$ of finite index. We define $Y(\Gamma) = \Gamma \backslash \mathcal{H}$. We will equip this with various interesting structures.

0.1 Recap of modular forms

Fix:

- $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$ with finite index (which we call the *level*)
- $k \in \mathbb{Z}$ (which we call the *weight*)

Then there exists a space $M_K(\Gamma)$ of *modular forms* which are functions $f : \mathcal{H} \to \mathbb{C}$ holomorphic, such that

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z) \; \forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma,$$

and a growth condition on the boundary.

There exists a subspace $S_k(\Gamma) \subset M_K(\Gamma)$ of *cusp forms.*

Fact (Basic)**.** *Both M_k and S_k are finite dimensional over $\mathbb{C}$.*

Any modular form has a *q-expansion,* let h be the least integer such that $\begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix} \in \Gamma$, then

$$f(z) = \sum_{n \geq 0} a_n q_h^n, \; a_n \in \mathbb{C}, \; q_h = e^{2\pi i z/h}.$$

1 Modular Curves as Riemann Surfaces

1.1 Modular curves as topological spaces

$\mathcal{H}$ has a topology (obviously) so $Y(\Gamma)$ gets a quotient topology (i.e., strongest topology such that $\pi : \mathcal{H} \to \Gamma(Y)$ is continuous). Quotient topology can be pretty nasty (for example $\mathbb{Q}$ acting on $\mathbb{R}$ by translation) - quotient can even be the indiscrete topology.

Proposition 1.1. *For any $\tau_1, \tau_2 \in \mathcal{H}$ there exists a neighbourhood $U_1 \ni \tau_1, U_2 \ni \tau_2$ such that if $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ satisfies $\gamma(U_1) \cap U_2 \neq \emptyset$, then $\gamma(\tau_1) = \tau_2$.*

Proof. See Proposition 2.1.1 of Diamond and Shurman. □

We say that $\mathrm{SL}_2(\mathbb{Z})$ acts *properly discontinuously on $\mathcal{H}$.*

Corollary 1.2. *$Y(\Gamma)$ is Hausdorff*

Proof. Let $P_1 \neq P_2$ be two points of $Y(\Gamma)$. Choose, $\tau_1, \tau_2 \in \mathcal{H}$ be lifting of P_1, P_2 respectively. Let U_1, U_2 be neighbourhoods of τ_1, τ_2 as in Proposition 1.1. We claim that $V_i = \pi(U_i)$ are open neighbourhoods of P_i such that $V_1 \cap V_2 = \emptyset$.

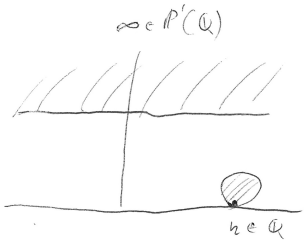
Suppose $V_1 \cap V_2 \neq \emptyset$, then $\pi^{-1}(V_1) \cap \pi^{-1}(V_2) \neq \emptyset$. Hence $\cup_{\gamma \in \Gamma} \gamma U_1 \cap \cup_{\gamma' \in \Gamma} \gamma' U_2 \neq \emptyset$. So there exists γ and γ' such that $\gamma U_1 \cap \gamma' U_2 \neq \emptyset$. This gives $(\gamma')^{-1}\gamma U_1 \cap U_2 \neq \emptyset$, which by Proposition 1.1 means $(\gamma')^{-1}\gamma\tau_1 = \tau_2$. This is a contradiction to the assumption that P_1 and P_2 are distinct point (hence τ_1, τ_2 are in different orbits) □

We are also interested in a slightly larger space $X(\Gamma)$, which is a compactification of $Y(\Gamma)$. As a set, we have

$$X(\Gamma) = Y(\Gamma) \cup \underbrace{C(\Gamma)}_{\text{"cusps" of } \Gamma}$$

$$C(\Gamma) = \Gamma \backslash \mathbb{P}^1(\mathbb{Q}).$$

Let $\mathcal{H}^* = \mathcal{H} \cup \mathbb{P}^1(\mathbb{Q})$. Give $\mathcal{H}^*$ a topology by extending the topology we have on $\mathcal{H}$.



If we define neighbourhoods of ∞ as $\{z : \mathrm{im}\, z > R\}$ for any $R \in \mathbb{N}$. Then so that the topology make sense, we defined neighbourhood of $x \in \mathbb{Q}$ as circles tangent to $\mathbb{R}$ at x. Actions on $\mathcal{H}^*$ are still properly discontinuous so $X(\Gamma)$ is Hausdorff.

Proposition 1.3. *$X(\Gamma)$ is compact.*

Proof. It suffices to find a compact subset of $\mathcal{H}^*$ mapping surjectively to $X(\Gamma)$. Let $D^* = \{\infty\} \cup \{z \in \mathcal{H} : \frac{1}{2} \leq \mathrm{re}\, z \leq \frac{1}{2}, |z| \geq 1\}$. A standard fact is that D^* contains a point of every $\mathrm{SL}_2(\mathbb{Z})$ orbit on $\mathcal{H}^*$. So if $\gamma_1, \ldots, \gamma_n$ are coset representative for $\Gamma \backslash \mathrm{SL}_2(\mathbb{Z})$, then $\cup_{i=1}^n \gamma_i D^*$ surjects onto $X(\Gamma)$. It is easy to check that D^* is compact, hence we are done. □

1.2 Riemann surfaces: recap

Definition 1.4. A *Riemann Surface* consists of the following data:

- A topological space X, (which is Hausdorff and second - countable)
- A collection $(U_i, V_i, \phi_i)_{i\in I}$, where $V_i \subset X$ are opens forming a cover of X, U_i are opens in $\mathbb{C}$ and $\phi_i : U_i \to V_i$ are homeomorphism, such that if $V_i \cap V_j \neq \emptyset$, the map $\phi_j^{-1} \circ \phi_i : U_i \cap \phi_i^{-1}(V_i \cap V_j) \to U_j \cap \phi_j^{-1}(V_i \cap V_j)$ is holomorphic.

Roughly: A Riemann surface is the least amount of structure on X needed to make sense of a function $X \to \mathbb{C}$ being holomorphic.

We will now show that $Y(\Gamma)$ and $X(\Gamma)$ have natural Riemann surface structures.

Definition 1.5. We say $P \in Y(\Gamma)$ is an *elliptic point* if for some (and hence any) $\tau \in \mathcal{H}$ lifting of P_1, $\mathrm{Stab}_{\overline{\Gamma}}(\tau) \neq \{1\}$, where $\overline{\Gamma}$ is the image of Γ in $\mathrm{PSL}_2(\mathbb{Z})$ (that is $\Gamma/\Gamma \cap \{\pm 1\}$)

If P is elliptic for Γ, then it maps to an elliptic point of $Y(\mathrm{SL}_2(\mathbb{Z}))$. One can see that there are only 2 of these (the orbits of i and $\rho = e^{2\pi i/3}$).

If P is not elliptic or a cusp, we can easily find a chart around P. Let τ be a lifting of P and apply Proposition 1.1 with $\tau_1 = \tau_2 = \tau$. Let $U = U_1 \cap U_2$, then U a neighbourhood of τ such that $\gamma U \cap U = \emptyset$ for any $\gamma \neq 1 \in \overline{\Gamma}$. Let V be the image of U in $Y(\Gamma)$, then $\phi = \pi/U$ is a homeomorphism $U \xrightarrow{\sim} V$.

If P is a elliptic, need to be a bit cleverer. Proposition 1.1 gives us a $U \ni \tau$ such that $U \cap \gamma U \neq \emptyset$ if and only if $\gamma \in \mathrm{Stab}_{\overline{\Gamma}}(\tau)$ (which has order 2 or 3). Choose $\delta \in \mathrm{SL}_2(\mathbb{C})$ shifting τ to 0 and $\overline{\tau}$ to ∞. Then $\mathrm{Stab}_{\overline{\Gamma}}(\tau)$ goes to a finite cyclic group of Mobius transformations fixing 0 and ∞, hence multiplication by $e^{2\pi i/n}$ with $n = 2$ or 3. Define the map $\mathrm{Stab}_{\delta\overline{\Gamma}\delta^{-1}}(0)\backslash\delta U \to U'$ by $z \mapsto z^n$, then this is a bijection. We define the coordinate chart to be the map $U' \to V$ as defined in the following map

$$\begin{array}{ccc} \mathrm{Stab}_{\delta\overline{\Gamma}\delta^{-1}}(0)\backslash\delta U & \longrightarrow & U' \\ \downarrow \sim & \swarrow \sim & \\ V \subset Y(\Gamma) & & \end{array}$$

Lastly, if P is a cusp, we argue similarly. Choose δ mapping P to ∞, $\mathrm{Stab}_{\delta\overline{\Gamma}\delta^{-1}}(\infty)$ is a group of translation, and $z \mapsto e^{2\pi i z/h}$ gives a local coordinates.

We have just proved that there exists a Riemann surface structure on $Y(\Gamma)$ and $X(\Gamma)$ such that $\pi : \mathcal{H} \to Y(\Gamma)$ is holomorphic. (Clearly the unique such structure).

1.3 Genus, ramification, Riemann-Hurwitz

Fact. *Riemann surfaces are smooth orientable 2-manifolds, and there are not many of these. Compacts connected ones all look like doughnuts with g holes.*

Definition 1.6. We define *genus* of a compact 2-manifold M, as the unique integer $g = g(M)$ such that $H^1(M, \mathbb{Z}) \cong \mathbb{Z}^{2g}$.

The genus is closely related to the *Euler Characteristic*, $\chi(M) = \sum_{i\geq 0}(-1)^i \operatorname{rk} H^i(M, \mathbb{Z})$. *If M is as in the Fact, then $H^0 \cong H^2 \cong \mathbb{Z}$ and $H^i = 0$ for $i \geq 3$, so $\chi(M) = 2 - 2g$.*

Proposition 1.7. *For $\Gamma = \mathrm{SL}_2(\mathbb{Z})$, the space $X(\Gamma)$ is isomorphic (as a Riemann surface, so in particular as 2-manifold) to $\mathbb{P}^1(\mathbb{C}) \cong S^2$.*

Proof. The "j-invariant" $j(z) = q^{-1} + 744 + 196884q + \dots$ is $\mathrm{SL}_2(\mathbb{Z})$ invariant and descend to a holomorphic map $X(\mathrm{SL}_2\,\mathbb{Z}) \to \mathbb{P}^1(\mathbb{C})$. It is bijective (counting zeroes using contour integration) so it has a holomorphic inverse. □

Convention: Unless otherwise stated all Riemann surfaces are assumed to be connected.

Recap: We want to find $g(X(\Gamma))$ for all Γ. We know that $X(\mathrm{SL}_2(\mathbb{Z}))$ has genus 0. We have that for all Γ, there is a map $X(\Gamma) \twoheadrightarrow X(\mathrm{SL}_2(\mathbb{Z}))$

Definition 1.8.

1. For $f : X \to Y$ a non-constant morphism, $P \in X$, the *ramification degree,* $e_P(f)$, is the unique integer $e \geq 1$ such that f "looks like $z \mapsto z^e$ locally". Note: points such that $e_P(f) > 1$ are *isolated.*
2. If X and Y are compact, the sum $\sum_{P \in f^{-1}(Q)} e_p(f)$ (which is independent of $Q \in Y$) is called the *degree* of f.

The degree of $X(\Gamma) \to X(\mathrm{SL}_2(\mathbb{Z}))$ is $[\mathrm{PSL}_2(\mathbb{Z}) : \overline{\Gamma}]$ (which is the number of preimages of a generic point of $X(\mathrm{SL}_2(\mathbb{Z}))$

Theorem 1.9 (Riemann - Hurwitz)**.** *For $f : X \to Y$ non-constant of degree N and X, Y compact, we have $2g(X) - 2 = N \cdot (2g(Y) - 2) + \sum_{P \in X}(e_P(f) - 1)$.*

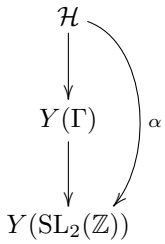
Corollary 1.10. *For any Γ, we have*

$$g(X(\Gamma)) = 1 + \frac{[\mathrm{PSL}_2(\mathbb{Z}) : \overline{\Gamma}]}{12} - \frac{\epsilon_2}{4} - \frac{\epsilon_3}{3} - \frac{\epsilon_\infty}{2}$$

where ϵ_2 is the number of elliptic points of order 2, ϵ_3 the number of elliptic points of order 3 and e_∞ the number of cusps.

Proof. We need to analyse the ramification of $X(\Gamma) \to X(\mathrm{SL}_2(\mathbb{Z}))$ at each $P \in X(\Gamma)$

- If $P \in Y(\Gamma)$ is not in the $\mathrm{SL}_2(\mathbb{Z})$-orbit of i or ρ.



  The map α is unramified at any τlifting a non elliptic point of $Y(\mathrm{SL}_2(\mathbb{Z}))$, so $e_P(f) = 1$

- If P maps to $[i]$: all such P are either non-elliptic or elliptic of order 2. If P is elliptic of order 2, then $Y(\Gamma) \to Y(\mathrm{SL}_2(\mathbb{Z})$ is locally an isomorphism at P so $e_P(f) = 1$. If P is non-elliptic, then local coordinate for $\mathrm{SL}_2(\mathbb{Z})$ is square of that for Γ, so $e_P(f) = 2$. We use the definition of the degree to count the number of points above $[i]$. We have $N = 1 \cdot \epsilon_2(\Gamma) + 2 \cdot (\text{number of non-elliptic points of } Y[\Gamma] \text{ above } [i])$. Hence, the number of non-elliptic points above $[i]$ is $(N - \epsilon_2)/2$. So

$$\sum_{P \in f^{-1}([i])} (e_P - 1) = \frac{N - \epsilon_2}{2}$$

- If P maps to $[\rho]$, (where $\rho = e^{2\pi i/3}$). Then $e_P(f) = \begin{cases} 1 & P \,\text{elliptic} \\ 3 & P \,\text{non} - \text{elliptic} \end{cases}$. We use the same argument as before, using the definition of degree, to get that the number of non-elliptic points above $[\rho]$ is $(N - \epsilon_3)/3$. Hence

$$\sum_{P \in f^{-1}([\rho])} (e_P - 1) = \frac{2(N - \epsilon_3)}{3}$$

- If P is a cusp: let h be the width of the cusp P (that is the integer such that $e^{2\pi iz/h}$ is a local coordinate for $X(\Gamma)$ at P). A local coordinate for $X(\mathrm{SL}_2(\mathbb{Z})$ at $[\infty]$ is $(e^{2\pi iz/h})^h$, so $e_p(f) = h$. Thus

$$\sum_{P \in f^{-1}([\infty])} (e_P - 1) = \left(\sum_{P \in f^{-1}([\infty])} e_P \right) - e_\infty = N - e_\infty$$

Putting all of this together, we get

$$\begin{aligned} 2g(X(\Gamma)) - 2 &= (-2)N + \frac{N - \epsilon_2}{2} + \frac{2(N - \epsilon_3)}{3} + (N - \epsilon_\infty) \\ g(X(\Gamma)) &= 1 + \frac{N}{12} - \frac{\epsilon_2}{4} - \frac{\epsilon_3}{3} - \frac{\epsilon_\infty}{2} \end{aligned}$$

□

Example. Let $\Gamma = \Gamma_0(11)$. We have that $N = 12$, $\epsilon_\infty = 2$ (they are $[0]$ and $[\infty]$), $\epsilon_2 = \epsilon_3 = 0$ (Exercise, c.f. D&S). Hence $g(X(\Gamma) = 1 + \frac{12}{12} - 0 - 0 - \frac{2}{2} = 1$.

Exercise. Show that the only primes p such that $g(X(\Gamma_0(p))) = 0$ are $\{2, 3, 5, 7, 13\}$.

Remark. For any g, there exists finitely many congruence subgroups Γ of $\mathrm{PSL}_2(\mathbb{Z})$ of genus g. (J.G. Thompson)

1.4 Sheaves and Riemann-Roch

Conjecture 1.11. *Let X be a topological space. Then you already know what a sheaf on X is.*

Now let X be a Riemann surface. We have $\mathcal{O}_X$ ("the structure sheaf") is defined by $\mathcal{O}_X(U)$ =holomorphic functions $U \to \mathbb{C}$. It is a sheaf of rings, so we can make sense of sheaves of $\mathcal{O}_X$-modules.

Definition 1.12. An *invertible sheaf* on X is a sheaf of $\mathcal{O}_X$-modules that is locally free of rank 1. (They are exactly the ones who have an inverse with respect to tensor product of $\mathcal{O}_X$-modules)

Fact. (For geometers) *Invertible sheaves are in bijection with line bundles with holomorphic structure.*

Now we specialise to the case of X is compact. We have a notion of meromorphic sections of invertible sheaves $\mathcal{F}$ (which are sections of $\mathcal{F} \otimes_{\mathcal{O}_X}$ {sheaf of meromorphic functions})

Theorem 1.13 (Riemann Existence Theorem)**.** *Any invertible sheaf on a compact Riemann Surface has a non-zero global meromorphic section.*

This implies that there is a notion of degree of an invertible sheaf, it is defined as the sum of the order of the vanishing of any non-zero L meromorphic global section. This is wee defined as the sum of zeroes and poles of a meromorphic function is 0.

We have $\deg(\mathcal{F} \otimes \mathcal{G}) = \deg \mathcal{F} + \deg \mathcal{G}$ and $\deg(\mathcal{F}^{-1}) = -\deg \mathcal{F}$. (Note that invertible sheaves are a group under $\otimes$ with $\mathcal{O}_X$ as identity, and deg is an group homomorphism to $\mathbb{Z}$)

Theorem 1.14 (Riemann - Roch)**.** *Let X be a compact Riemann Surface, $\mathcal{F}$ an invertible sheaf on X. Then*

1. *$\mathcal{F}(X) =: H^0(X, \mathcal{F})$ is finite dimensional over $\mathbb{C}$*
2. *$\dim H^0(X, \mathcal{F}) - \dim H^0(X, \Omega \otimes \mathcal{F}^{-1}) = 1 - g + \deg \mathcal{F}$, where Ω is the sheaf of holomorphic differentials on X.*

Note that if $\deg(\mathcal{F}) < 0$, then $\mathcal{F}$ has no non-zero global sections, so if $\deg \mathcal{F}$ is large, $H^0(X, \Omega \otimes \mathcal{F}^{-1}) = 0$, hence we get a formula for $\dim H^0(X, \mathcal{F})$. (Note that $\dim H^0(X, \Omega) = g(X)$ by setting $\mathcal{F} = \mathcal{O}_X$, furthermore $\deg \Omega = 2g - 2$ by taking $\mathcal{F} = \Omega$)

[**Aside**: There exists a cohomological theorem for sheaves on Riemann surfaces for which $H^0(X, \mathcal{F})$ is sections. the Riemann - Roch is a combination of 2 things:

- a formula for $\chi(\mathcal{F}) = \sum_{i \geq 0} (-1)^i \dim H^i(X, \mathcal{F})$
- Serre duality: $H^i(X, \mathcal{F}) = H^{1-i}(X, \Omega \otimes \mathcal{F}^{-1})^*$. (This is why sometime Ω is referred as the "dualising sheaf"]

1.5 The Katz sheaf

Let $X = X(\Gamma)$ for some Γ, and choose $k \in \mathbb{Z}$.

Definition 1.15. Let ω_k be the sheaf defined by $\omega_k(V) = \{\text{holomorphic functions on } \pi^{-1}(V) \subset \mathcal{H}^* \text{ satisfying } f(\gamma z) = j(\gamma, z)^k f(z) \text{ for all } \gamma \in \Gamma\}$.

This is a sheaf of $\mathcal{O}_{X(\Gamma)}$-modules. If k is odd and $-1 \in \Gamma$ it is the zero sheaf, we now assume that we are not in this case.

Theorem 1.16.

1. *ω_k is invertible*
2. *$\omega_2 = \Omega_{X(\Gamma)}(\text{cusps})$*

Remark. Here, for $\mathcal{L}$ an $\mathcal{O}_X$-module sheaf and $D = \sum n_i P_i$ is a divisor (formal $\mathbb{Z}$-linear combination of points), we define $\mathcal{L}(D)(U) = \{\text{meromorphic sections } x \text{ of } \mathcal{L} \text{ over } U \text{ with } \operatorname{div}(x) + D \geq 0\}$. For example:

- $L(P) =$ "allow simple poles at P"
- $L(-P) =$ "sections vanishing at P"

Proof.

1. This is a case by case check. We just need to show it on a open neighbourhood of every $P \in X(\Gamma)$. That is we want to show that for every $P \in X(\Gamma)$ there exists a neighbourhood $V \ni P$ and $b \in \omega_k(V)$ such that $\omega_k(V) = \mathcal{O}_X(V) \cdot b$.

   For P non-elliptic, not cusp, we can find $V \ni P$ open such that $\pi^{-1}(V) = \sqcup_{\gamma \in \overline{\Gamma}} \gamma U$ and $\omega_k(V) \cong \mathcal{O}_{\mathcal{H}}(U) \cong \mathcal{O}_X(V)$.

   Other cases: Choose $\tau \in \mathcal{H}^*$ to be a lifting of P, $U \subset \mathcal{H}^*$ open such that U is fixed by $\operatorname{stab}_\Gamma(\tau)$ and

   $$\pi^{-1}(V) = \coprod_{\gamma \in \overline{\Gamma}/\operatorname{stab}_\Gamma(\tau)} \gamma U$$

   where $V = \pi(U)$. So $\omega_k(V) = \{f : U \to \mathbb{C} \text{ holomorphic and weight } k \text{ invariant under } \operatorname{Stab}_\Gamma(\tau)\}$ while $\mathcal{O}_X(V) = \{f : U \to \mathbb{C} \text{ holomorphic and weight 0 invariant under } \operatorname{Stab}_\Gamma(\tau)\}$. So if $\operatorname{Stab}_\Gamma(\tau) = 1$ we are done (take $b = 1$), or more generally if the weight k action of $\operatorname{Stab}_\Gamma(\tau)$ is trivial. (Happens if τ is elliptic and k is divisible by the order of $\operatorname{Stab}_\Gamma(\tau)$)

   For elliptic points: if τ is elliptic, conjugate it onto $z = 0$ as before so $\operatorname{Stab}_\Gamma(\tau) =$cyclic group of rotation with order n, say. A function $U \to \mathbb{C}$ is weight k invariant under this group if and only if $f(z) = z^a g(z^n)$ where a is the least non negative integer congruent to $k \mod n$ and some holomorphic function g. So $z \mapsto z^a$ is a local basis.

   For cusps: if τ is a cusp, and the cusp is regular or the weight is even, the action of $\operatorname{Stab}_\Gamma(\tau)$ in weight k and weight 0 coincides, so $b = 1$ works.

   If τ is an irregular cusps, k odd, (without loss of generality $\tau = \infty$) then $\mathcal{O}_X(V) = \{f : U \to \mathbb{C} \text{ holomorphic such that } f(z + h) = f(z)\}$ while $\omega_k(V) = \{f : U \to \mathbb{C} \text{ holomorphic such that } f(z + h) = -f(z)\}$ (where h is the height of the cusp). Then $z \mapsto e^{i\pi z/h}$ is a local basis.

2. The isomorphism is $f \mapsto f(z)dz$. Clearly if is a bijection $\mathcal{O}_{\mathcal{H}}(\mathcal{H}) \to \Omega^1_{\mathcal{H}}(\mathcal{H})$ and it commutes with Γ-action if we put weight 2 action on $\mathcal{O}_{\mathcal{H}}$. Passing to Γ-invariants $\omega_2|_{Y(\Gamma)} = \Omega^1_{Y(\Gamma)}$.

   We need to show that sections of ω_2 extending to corresponding cusps correspond to differentials with simple poles. It suffices to consider the case $\tau = \infty$. Sections of Ω^1 near ∞ are $f(q)dq$. But $q = e^{2\pi iz/h}$ implies $dq = \frac{2\pi i}{h} e^{2\pi iz/h} dz$, i.e., dz is a scalar times $\frac{dq}{q}$. Hence "$\mathcal{O}_X dz = \mathcal{O}_X \frac{dq}{q} = \mathcal{O}_X(\infty)dq$" (over a neighbourhood $V \ni \infty$)

□

Obviously $H^0(X(\Gamma), \omega_k) = M_k(\Gamma)$.

Proposition 1.17. *Let*

$$r = \text{lcm}\left(\text{order of } \Gamma\text{−stabaliser of elliptic points}, \left\{ \begin{array}{cc} 2 & \text{if } \exists \text{ irregular cusp} \\ 1 & \text{else} \end{array} \right\}\right)$$

Note that $1 \leq r \leq 12$. *Then* $\omega_{k+r} \cong \omega_k \otimes \omega_r$ *for all* $k \in \mathbb{Z}$. *In particular if* $r = 1$ *then* $\omega_k = (\omega_1)^{\otimes k}$ *for all* k.

Proof. For $k = r$ all the local bases b in Theorem 1.16 were 1 and bases of ω_k for general k only depended on k mod r. So local basis for ω_{k+r} is equal to the product of ones for ω_k and ω_r □

Definition 1.18. If $r = 1$ above (i.e., Γ has no elliptic points, it does not contain -1 and all cusps are regular), we say Γ is *neat*. Then $\omega_k = \omega_1^{\otimes k}$, so $\omega = \omega_1$ is obviously important. Call this the *Katz sheaf*.

Corollary. *If* Γ *is neat, then for* $k \geq 2$ *we have* $\dim M_k(\Gamma) = (k-1)(g-1) + \frac{k}{2}\epsilon_\infty$.

Proof. We have

$$\begin{aligned} \deg \omega &= \frac{1}{2}\deg(\omega^{\otimes 2}) \\ &= \frac{1}{2}(\deg \Omega + \epsilon_\infty) \\ &= \frac{1}{2}(2g - 2 + \epsilon_\infty). \end{aligned}$$

So if $k \geq 2$, $\deg \omega^{\otimes k} > 2g - 2$ and Riemann - Roch gives

$$\begin{aligned} \dim H^0(X(\Gamma), \omega^k) &= k \cdot (g - 1 + \frac{\epsilon_\infty}{2}) - g + 1 \\ &= (k-1)(g-1) + \frac{k}{2}\epsilon_\infty \end{aligned}$$

□

There exists similar (but messier) formulae in the non-neat case (c.f. D-S chapter 3)

Example. Let $\Gamma = \Gamma_1(5)$, this is neat ($\Gamma_1(N)$ is neat if and only if $N \geq 5$), $g = 0$ and $\epsilon_\infty = 4$. So $\dim M_k(\Gamma) = k+1$ for $k \geq 2$. For $k = 1$ we need to worry about $H^0(X(\Gamma), \Omega^1 \otimes \omega^{-1})$, but $\deg \Omega^1 = 2g - 2 = -2$, $\deg \omega = 1$. So $\Omega^1 \otimes \omega^{-1}$ had $\deg -1$.

If you try to do this for $\Gamma_1(23)$ if fails, $\deg \Omega^1 \otimes \omega^{-1}$ is 0. So dimension of Wight 1 form spaces lie much deeper.

2 Modular Curves as Algebraic Curves

2.1 Modular Curves over $\mathbb{C}$

Theorem 2.1.

1. *The $\mathbb{C}$-points of a smooth connected projective algebraic curve over $\mathbb{C}$ are canonically a Riemann surface, $X \mapsto X^{\mathrm{an}}$*
2. *Every compact Riemann surface is X^{an} for a unique X*
3. *There exists an equivalence of categories between (locally free sheaves of $\mathcal{O}_X$-modules) $\cong$ (locally free sheaves of $\mathcal{O}_{X^{\mathrm{an}}}$-modules), preserving global sections*

Remark. 1. is basically the implicit function theorem. We'll see later a bit about the proof of 2. . 3. is Serre's "GAGA" theorem.

The functors are on one hand $\mathcal{F} \mapsto \mathcal{O}_{X^{\mathrm{an}}} \otimes_{\mathcal{O}_X} \mathcal{F}$, and on the other hand $\mathcal{F} \mapsto$ (subsheaf of $\mathcal{F}$ whose sections over U are elements of $\mathcal{F}(U)$ extending to meromorphic sections on X).

Hence for any Γ there's an algebraic variety $X(\Gamma)_{\mathbb{C}}$ and invertible sheaves ω_k on it such that $M_k(\Gamma) = H^0(X(\Gamma)_{\mathbb{C}}, \omega_k)$.

Here's an alternative, nicer, construction.

Theorem 2.2.

$$X(\Gamma)_{\mathbb{C}} = \mathrm{Proj}\left(\bigoplus_{k\geq 0} M_k(\Gamma)\right).$$

Remark. C.f. Hartshorne Algebraic Geometry Chapter 2 for the definition/construction of Proj.

Proof. One knows that for any Noetherian graded $\mathbb{C}$-algebra $S_\bullet$, with $S_0 = \mathbb{C}$, $\mathrm{Proj}(S_\bullet) = \mathrm{Proj}(S_{n\bullet})$ for any $n \geq 1$. (Where $S_{n\bullet}$ = the subring $\oplus_{k\geq 0} S_{nk}$). Choose n to be r from Proposition 1.17, so

$$S_{n\bullet} = \oplus_k H^0\left(X(\Gamma), \omega_n^{\otimes k}\right).$$

We now quote a standard fact in algebraic geometry: Invertible sheaves of positive degree on curves are ample, so their sections give an embedding in projective space. □

Remark. In fact the same argument can be used to prove Theorem 2.1 part 2. : take any ample invertible sheaf on a Riemann surface and get an embedding in $\mathbb{P}^n$ for $n \gg 0$.

2.2 Descending the base field

Question: Does there exists an algebraic curve over some number field K such that we get $X(\Gamma)_{\mathbb{C}}$ by base extension?

Let's think a bit what this means:

- Clearly not all varieties over $\mathbb{C}$ are definable over number fields. For example $Y^2 = X^3 + X + \pi$, this is not defined over any number field, as its j invariant is $\frac{6192}{27\pi^2+4}$. But we need to be careful as $\pi Y^2 = X^3 + X$ is defined over $\mathbb{Q}$ (it is isomorphic to $Y^2 = X^3 + X$)
- Even if descends exists they might not be unique. For example, $\mathbb{P}^1_{\mathbb{Q}}$ and $\{X^2 + Y^2 + 2Z^2 = 0\} \subset \mathbb{P}^2_{\mathbb{Q}}$ become isomorphic over $\mathbb{C}$.

So we need to ask, is there a descend to a number field that "means something"?

The curves - fields correspondence

There is a bijection, for any field k, {smooth geometrically connected algebraic curves over k}$\leftrightarrow$ {field extensions K/k of transcendence degree 1 containing no algebraic extensions of k}. The bijection is given by $X \mapsto k(X)$, the field of rational functions on X.

So for a curve$X$ over $\mathbb{C}$ we have {models of X over $k \subseteq \mathbb{C}$} $\leftrightarrow$ {subfields L of $\mathbb{C}(X)$ generating it over $\mathbb{C}$ but with $L \cap \mathbb{C} = k$}.

So we want to look for nice subfields of $\mathbb{C}(X(\Gamma)_{\mathbb{C}}) = \{$meromorphic modular functions of weight 0 and level $\Gamma\}$.

Theorem 2.3. *Let $N \geq 2$*

1. $\mathbb{C}(X_0(N)) = \mathbb{C}(j(z), j(Nz))$
2. *The minimal monic polynomial of $j(Nz)$ over $\mathbb{C}(j(z))$ lies in $\mathbb{Z}[j][Y] \subseteq \mathbb{C}(j)[Y]$, and is $\Phi_N(j, Y)$ for Φ_N symmetric.*
3. *If $N = p$ is prime, $\Phi_p(X, Y) \equiv (Y^p - X)(Y - X^p) \mod p$.*

In particular $X_0(N)_{\mathbb{C}}$ has a model over $\mathbb{Q}$ whose function field is $\mathbb{Q}(j(z), j(Nz))$

Proof. (cf. Mine's notes "MFMF" pg 90-92)

1. Clearly $j(Nz) \in \mathbb{C}(X_0(N))$, so $\mathbb{C}(j(z), j(Nz)) \subseteq \mathbb{C}(X_0(N))$. Over $\mathbb{C}(j)$, the right hand side has degree $[\mathrm{PSL}_2(\mathbb{Z}) : \overline{\Gamma_0(N)}] = [\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(N)] =: \mu$. So if we show that $j(Nz)$ has degree μ over $\mathbb{C}(j)$, then part 1. follows.

   Let $\gamma_1, \ldots, \gamma_\mu$ be such that $\mathrm{SL}_2 \mathbb{Z} = \coprod_{i=1}^{m} \Gamma_0(N)\gamma_i$ (without loss of generality $\gamma_1 = 1$). Consider the functions $j(N\gamma_i z)$. All Galois conjugate to $j(Nz)$ over $\mathbb{C}(j)$ (via the automorphism $z \mapsto \gamma_i z$ of $\mathbb{C}(\mathcal{H})$). If we can show that they are distinct then part 1. follows by Galois theory. So suppose $j(N\gamma_i z) = j(N\gamma_k z)$ for some $1 \leq i, k \leq \mu$, for all $z \in \mathcal{H}$. Then

$$j\left(\underbrace{\begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix} \gamma_k \gamma_i^{-1} \begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix}^{-1}}_{:=A} z\right) = j(z) \ \forall z \in \mathcal{H}.$$

   By a question from sheet 1. this forces $\pm A \in \mathrm{PSL}_2(\mathbb{Z})$, so $\gamma_k \gamma_i^{-1} \in \Gamma_0(N)$, hence $i = k$.

2. From part 1. we know the monic minimal polynomial of $j(Nz)$ is $\prod_{i=1}^{n}(Y - j(N\gamma_i z))$. The coefficients are symmetric polynomials in $\{j(N\gamma_i z)\}$, so they are all holomorphic on $\mathcal{H}$. Since they are also rational functions in $j(z)$, they must be polynomials in $j(z)$.

   To control coefficients we use q-expansions. We know that $j(z) = q^{-1} + 744 + \cdots \in q^{-1} + \mathbb{Z}[[q]]$. Moreover, we can choose the γ_j such that $j(N\gamma_i z) = j\left(\frac{az+b}{d}\right)$ for some $a, b, d \in \mathbb{Z}$ such that $ad = N$. So $j(N\gamma_i z) \in \mathbb{Z}[\zeta_N]((q^{\frac{1}{N}}))$ (where $\zeta_N = e^{2\pi i/N}$). So the coefficients of $\Phi_N(j, Y)$ (as a polynomial in Y) have q-expansion in $\mathbb{Z}[\zeta_N]((q^{\frac{1}{N}})) \cap \mathbb{C}((q)) = \mathbb{Z}[\zeta_N]((q))$.

   Claim. These coefficients are actually in $\mathbb{Z}[\zeta_N][j]$

   Let $P = \sum_{i=1}^{k} b_i j^i \in \mathbb{Z}[j]$ have q-expansion in $R((q))$ for some $R \subseteq \mathbb{C}$ a subring. Inspecting lowest term of q-expansion, we see that $b_k \in R$. By induction on degree, we have $b_i \in R$ for all i. So $\Phi_N(X, Y) \in \mathbb{Z}[\zeta_N][X, Y]$. Write $\Phi_N(X, Y) = \sum_{r,s} c_{rs} X^r Y^s$, substitute in q-expansions of $j(z), j(Nz)$ and equate coefficients. We get equations for $\{c_{rs}\}$, linear with $\mathbb{Q}$-coefficients. We know $c_{r\mu} = \begin{cases} 1 & r = 0 \\ 0 & r > 0 \end{cases}$ and that there is a unique solution over $\mathbb{C}$. So solution must be $\mathrm{Gal}(\mathbb{Z}[\zeta_N]/\mathbb{Z})$ invariant, i.e., $\Phi_N(X, Y) \in \mathbb{Z}[X, Y]$.

   To prove symmetry: $\Phi_N(j(z), j(Nz)) = 0$ for all z. This implies $\Phi_N\left(j\left(\frac{1}{Nz}\right), j\left(\frac{-N}{Nz}\right)\right) = 0 \, \forall z \in \mathcal{H}$. Rearranging, this gives $\Phi_N(j(Nz), j(z)) = 0$. So $\Phi_N(Y, X)$ is a multiple of $\Phi_N(X, Y)$. Hence $\Phi_N(X, Y) = c\Phi_N(Y, X)$ for some $c^2 = 1$. Since $N \geq 2$, we can't have $c = -1$ as this would force Φ_N to be a multiple of $X - Y$, hence $c = 1$.

3. Note that $\Phi_p(j(z), Y)$ has q-expansion

$$(Y - j(pz)) \left(\prod_{i=1}^{p-1} \left(Y - j\left(\frac{z+i}{p} \right) \right) \right).$$

Now q-expansions of functions $j\left(\frac{z+i}{p}\right)$ are all congruent modulo a unique prime $\mathfrak{p}|p$ of $\mathbb{Z}[\zeta_p]$, so modulo $\mathfrak{p}$ reduction $\phi_p(j, Y)$ is

$$\begin{aligned} (Y - j(z)) \left(Y - j\left(\frac{z}{p} \right) \right)^p &\equiv (Y - j(z)^p) \left(Y^p - j\left(\frac{z}{p} \right)^p \right) \\ &\equiv (Y - j(z)^p) \left(Y^p - j(z) \right) \mod \mathfrak{p}. \end{aligned}$$

This forces some congruence for Φ_p as a polynomial.

□

Remark.

1. $Y_0(N)$ is <u>not</u> the curve in $\mathbb{A}^2$ defined by $\Phi_N(X, Y) = 0$. It is <u>birationally equivalent</u> to it but not generally isomorphic; $\{\Phi_N(X, Y) = 0\}$ is generally <u>singular</u>.
2. Φ_N's have <u>huge</u> coefficients. For example

$$\Phi_2(X, Y) = X^3 + Y^3 - X^2Y^2 + 1488XY(X + Y) - 162000(X^2 + Y^2)$$

$$+40733375XY + 8748000000(X + Y) - 137464000000000$$

3. Note that mod p relations of Φ_p defines a <u>reducible</u> curve, we get two copies of $\mathbb{P}^1$ intersecting.

We define $X_0(N)_{\mathbb{Q}}$ as the unique smooth projective curve over $\mathbb{Q}$ with function field $\mathbb{Q}(X, Y)/\Phi_N(X, Y)$.

Theorem 2.4. *There is a sheaf $\omega_{k,\mathbb{Q}}$ on $X_0(N)_{\mathbb{Q}}$ whose base-extension to $\mathbb{C}$ is ω_k.*

Proof. As $-1 \in \Gamma_0(N)$, ω_k is only non-zero for $k \in 2\mathbb{Z}$. We know $\omega_2 \cong \Omega^1_{X_0(N)_{\mathbb{C}}}(\text{cusps})$. More generally we always have $\omega_{2k} \cong \left(\Omega^1_{X_0(N)_{\mathbb{C}}}\right)^{\otimes k}(D_k)$ where D_k is a $\mathbb{Z}$-linear combination of the divisors: (cusps), (elliptic points of order 2), and (elliptic points of order 3).

Claim. These 3 divisors descend to $X_0(N)_{\mathbb{Q}}$.

For (cusps) this is clear: the map $X_0(N) \to X_0(1)$ is defined over $\mathbb{Q}$ (as $j \in \mathbb{Q}(j(z), j(Nz))$). Cusps are exactly the preimages of the $\mathbb{Q}$-points $(\infty) \in X_0(1)$.

For elliptic points we need to be a bit careful: {elliptic points of $X_0(N)_{\mathbb{C}}$ of order 2} = {preimages of $i \in X_0(1)$ where the projection map $X_0(N) \to X_0(1)$ is unramified}. Ramification degree is <u>Galois invariant</u> so we are done. Note $j(i) = 1728$ and $j(\rho) = 0$, hence $i, \rho \in X_0(1)(\mathbb{Q})$.

So we can define

$$\omega_{2k,\mathbb{Q}} = \left(\Omega^1_{X_0(N)_{\mathbb{Q}}}\right)^{\otimes k}(D_k).$$

□

Corollary 2.5. *For any $k \geq 2$ even, any $N \geq 1$, the spaces $S_k(\Gamma_0(N))$ and $M_k(\Gamma_0(N))$ have bases consisting of forms with q-expansions in $\mathbb{Q}[[q]]$.*

Proof. We only give the argument for M_k, as the argument for S_k is similar. We have

$$\begin{aligned} M_k(\Gamma_0(N)) &= H^0(X_0(N)_{\mathbb{C}}, \omega_k) \\ &= \mathbb{C} \otimes_{\mathbb{Q}} H^0(X_0(N)_{\mathbb{Q}}, \omega_{k,\mathbb{Q}}). \end{aligned}$$

Claim. The image of $H^0(X_0(N)_{\mathbb{Q}}, \omega_{k,\mathbb{Q}})$. is a function of q-expansions with in $(2\pi i)^{k/2}\mathbb{Q}[[q]]$.

Any meromorphic section of ω_k is in $\mathbb{Q}(j(z), j(Nz)) \cdot (dj)^{\otimes k/2}$. Now $dj = j'(z)dz$, say $j(z) = J(q)$, then $dj = J'(q)2\pi i q dz$. So any meromorphic sections of ω_k lands in $(2\pi i)^{k/2}\mathbb{Q}((q))$.

□

3 Modular Curves as Moduli Spaces

3.1 Lattices and Level Structures

Recall: If Λ is a lattice in $\mathbb{C}$ (a discrete subgroup isomorphic to $\mathbb{Z}^2$), Λ is homothetic to a lattice of the form $\Lambda_\tau := \mathbb{Z} + \mathbb{Z}\tau$ for some $\tau \in \mathcal{H}$, and τ is uniquely determined modulo $\mathrm{PSL}_2(\mathbb{Z})$.

$Y(\mathrm{SL}_2(\mathbb{Z})) = \{\text{homothety classes of lattices}\} = \{\text{isomorphism classes of elliptic curves over } \mathbb{C}\}$.

Exercise.

1. For any $N \geq 2$ there exists a bijection between $Y_0(N) \cong \{\text{pairs of } (\Lambda, C)$: Λ a lattice, C a cyclic subgroup of $\mathbb{C}/\Lambda$ of order N, where $(\Lambda, C) \cong (\Lambda', C')$ if there exists an isomorphism $\mathbb{C}/\Lambda \cong \mathbb{C}/\Lambda'$ sending C to $C'\}$. The isomorphism is defined by $[\tau] \mapsto \left(\mathbb{Z} + \mathbb{Z}\tau, \frac{1}{N}\mathbb{Z}\right)$.

2. For any $N \geq 2$ there exists a bijection between $Y_1(N) \cong \{\text{pairs } (\Lambda, P) : \Lambda \text{ a lattice, } P \text{ a point of exact order } N$, modulo the equivalence relation $(\Lambda, P) \sim (\Lambda', P')$ if there exists an isomorphism $\mathbb{C}/\Lambda \cong \mathbb{C}/\Lambda'$ sending P to $P'\}$

Note that in part 2. (Λ, P) is always equivalent to $(\Lambda, -P)$. In part 1. we have lots more exceptional cases coming from elliptic points.

We have a natural question: if $x \in Y_0(N)$ is a $\mathbb{Q}$-point, does (E, C), $E = \mathbb{C}/\Lambda$, descend to $\mathbb{Q}$? This is the right sort of question to ask to understand modular curves over number fields. (This actual question is vacuous for $N \gg 0$, but we don't know that yet)

3.2 Moduli spaces and representable functors

All rings are commutative and unital. We have the categories: Rings, R-Alg for a ring R, and Sets. (We do not worry about foundational issues). "Most sets that come up naturally in algebraic geometry are functors Ring$\to$Set (or R-Alg$\to$Set)".

Example.

1. Points of varieties over schemes.

2. Classes of varieties or structures on varieties.

A lot of the fun of algebraic geometry arises from the fact that instances of 2. are often 1. in disguise. These are moduli spaces.

Some properties of functors and representable functions

Let C be a category ("locally small" - homomorphism between any two objects are a set). Then $\mathrm{Hom}(X, -)$ is a functor $C \to \mathrm{Set}$, which we denote by h^X. A functor $\mathcal{F} : C \to \mathrm{Set}$ is *representable* if there exists an isomorphism of functors $\mathcal{F} \cong h^X$ for some $X \in \mathrm{Ob}(C)$. How do we specify the isomorphism $\mathcal{F} \cong h^X$?

Note. h^X has a canonical element: namely id_X.

So we need to know a corresponding element of $\mathcal{F}(X)$, as $h^X(X) \cong \mathcal{F}(X)$. Having specified a $\phi : \mathcal{F}(X)$ corresponding to id_X, this determines an element of $\mathcal{F}(Y)$ for every homomorphism $\alpha : X \to Y$, i.e., take $\mathcal{F}(\alpha)(\phi)$.

Proposition 3.1 (Yoneda's Lemma)**.** *This construction is a bijection:* $\{\text{natural transformations } h^X \to \mathcal{F}\} \xrightarrow{\sim} \mathcal{F}(X)$, *for any* $\mathcal{F} : C \to \mathrm{Set}$ *and* $X \in \mathrm{Ob}(C)$.

Remark. WE have discussed covariant functors, but we get the same for contravariant functors by replacing C with C^{opp})

So if $\mathcal{F}$ is representable, the bijection $\mathcal{F}(X) \cong h^X(Y)$ is determined by a $\phi \in \mathcal{F}(X)$; we are saying that for every $Y \in \mathrm{Ob}(C)$ and every $\psi \in \mathcal{F}(Y)$, there exists a unique homomorphism $\alpha : X \to Y$ such that $\alpha(\phi) = \psi$. We say (X, ϕ) represents $\mathcal{F}$. Hence ϕ is essential part of the data.

Example. Let $C = \underline{\text{Ring}}$

- $\mathcal{F}(R) = R$ (the forgetful functor). This is represented by $(\mathbb{Z}[T], T)$, i.e., for any ring R, $r \in R$, there exists a unique $\alpha : \mathbb{Z}[T] \to R$ such that $\alpha(T) = r$.
- $\mathcal{F}(R) = R^*$ is represented by $(\mathbb{Z}[T, T^{-1}], T)$
- $\mathcal{F}(R) = \{n\text{th root of unity in } R\}$ is represented by $(\mathbb{Z}[T]/(T^n - 1), T)$.
  Note. "primitive nth root of unity" is not a functor on R

A Non-Example. Let $C = \underline{\text{Ring}}$. Consider $\mathcal{F}(R) = (\text{squares in } R)$. This is $\underline{\text{not}}$ representable

Proof. Suppose $\mathcal{F}$ is represented by (A, a), some ring A and $a \in A$ with $a^2 = b$ for some $b \in A$. Then for any ring S and element $s \in S$ such that s is a square, there needs to exists a unique homomorphism $\alpha : A \to S$ such that $\alpha(a) = s$. But take $S = \mathbb{Z}[T]$, $s = T^2$, so there exists unique $\alpha : A \to \mathbb{Z}[T]$ with $\alpha(a) = T^2$, hence $\alpha(b) = \{\pm T\}$. Let $\sigma : S \to S$ be $T \mapsto -T$, note that $\sigma(s) = s$. So $\sigma \circ \alpha \in \text{Hom}(A, S)$ also sends a to s, but $\sigma \circ \alpha \neq \alpha$ as $(\sigma \circ \alpha)(b) \neq \alpha(b)$. This contradicts uniqueness of α □

The moral of this example: Automorphism are $\underline{\text{bad}}$ for representability.

3.3 Elliptic curves over general base schemes

We want to make sense of "elliptic curves over S", where S a scheme.

Definition 3.2. Let S be a scheme. An *elliptic curve* over S is a scheme $\mathcal{E}$ with a morphism $\pi : \mathcal{E} \to S$ (an S-scheme) such that π is flat and proper, and all fibres are smooth genus 1 curves, given with a section "O": $S \to \mathcal{E}$.

Example. In Silverman's book, there is the equation $Y^2 + XY = X^3 - \frac{36}{j-1728}X - \frac{1}{j-1728}$. The associated homogeneous cubic $Y^2Z + XYZ = X^3 - \frac{36}{j-1728}XZ^2 - \frac{1}{j-1728}Z^3$ is a subscheme of $\mathbb{P}^2/R$, where R is the ring $\mathbb{Z}[j, j^{-1}, (j - 1728)^{-1}]$. This is an elliptic curve over Spec$R$. The discriminant is $\Delta = j^2/(j - 1728)^3$.
Think of this as a $\underline{\text{family of elliptic curves}}$, one for every $j \neq 0, 1728$, varying in an "algebraic way".

For $\mathcal{E}$ over S as above, $E(S) = \text{Hom}_{S-\text{sch}}(S, \mathcal{E})$ =sections of $\pi : \mathcal{E} \to S$ picking out a point on each fibre.
Warning: If $P \in \mathcal{E}(S)$ has order N, i.e., $N \cdot P = 0$ and $M \cdot P \neq 0$ for $1 \leq M < N$, it is not necessarily true that P_x has order N on $\mathcal{E}_x$ for every $x \in S$. (E.g., if $\mathcal{E}$ over Spec$(\mathbb{Z}_p)$ can have points of order P reduction mod p to 0 at closed points of Spec $\mathbb{Z}_p$).

Proposition 3.3. *If $\mathcal{E}$ over S is an elliptic curve, then $\mathcal{E}$ has a Weierstrass equation $\underline{\text{locally on } S}$. That is, there exists a covering $\coprod U_i \to S$ in Zariski topology such that $\mathcal{E}|_{U_i}$ has a Weierstrass equation for all i.*
More precisely, we'll "show" the following: $\omega_{\mathcal{E}/S} := \pi_*(\Omega^1_{\mathcal{E}/S})$ is an invertible sheaf on S, and any local basis ω of $\omega_{\mathcal{E}/S}$ (over some $U \subset S$ open) determines a Weierstrass equation over U. If 2 is invertible on S, we can do this in such a way that $\omega = -\frac{dx}{2y}$.

Proof (Sketch). The invertibility of $\omega_{\mathcal{E}/S}$ comes from a calculation in sheaf cohomology, c.f., pg53 of Mumford "Abelian Varieties".
Now, given U and ω a basis of $\pi_*(\Omega^1_{\mathcal{E}/U})$, this gives local parameter on $\mathcal{E}$ at 0 such that $\omega = dT(1 + \text{higher order terms})$. T is called a "local parameter adapted to ω". Now $\pi_*(\mathcal{O}_\mathcal{E}(2(0)))$ is locally free of rank 2 over U. Assume $U = \text{Spec}(A)$ affine, then $\pi_*(\mathcal{O}_\mathcal{E}(2(0)))$ is $A \cdot (1, x)$ where $x = \frac{1}{T^2}(1 + \dots)$. Similarly:

- $\pi_*(\mathcal{O}_\mathcal{E}(3(0)))$ is $A(1, x, y)$ where $y = \frac{1}{T^3}(1 + \dots)$,
- $\pi_*(\mathcal{O}_\mathcal{E}(4(0)))$ is $A(1, x, y, x^2)$
- $\pi_*(\mathcal{O}_\mathcal{E}(5(0)))$ is $A(1, x, y, x^2, xy)$

Note $y^2 - x^3 \in \pi_*(\mathcal{O}_\mathcal{E}(5(0))$, so $y^2 - x^3 \in A(1, x, y, x^2, xy)$ and that's a Weierstrass equation over $A[x, y]$. Moreover $dx = \frac{-2dT}{T^3} + \dots$ and $y = \frac{1}{T^3} + \dots$, so $\frac{-dx}{2Y} = \omega \mod TdT$. (We don't have such a nice characterization of the Weierstrass equation if 2 is not invertible on S. □

Definition 3.4. For S a scheme, $\alpha, \beta \in \Gamma(S, \mathcal{O}_S)$, let $E(\alpha, \beta)$ be the subscheme of $\mathbb{P}^2_S$ defined by $Y^2Z + \alpha XYZ + \beta YZ^2 = X^3 + \beta X^2 Z$, and let $\Delta(\alpha, \beta) = -\beta^3(\alpha^4 - \alpha^3 + 8\alpha^2\beta - 36\alpha\beta + 16\beta^2 + 27\beta)$ be its discriminant.

If $\Delta(\alpha, \beta) \in \Gamma(S, \mathcal{O}_S)^*$ this is an elliptic curve over S. Note that $P = (0 : 0 : 1) \in E(S)$ and we calculate

- $P = (0 : 0 : 1)$
- $2P = (-\beta : \beta(\alpha - 1) : 1)$
- $3P = (1 - \alpha : \alpha - \beta - 1 : 1)$
- $-P = (0 : -\beta : 1)$
- $-2P = (-\beta : 0 : 1)$
- $-3P = (1 - \alpha : (\alpha = 1)^2 : 1)$

This means that P does not have order $1, 2$ or 3 in any fibre.

Proposition 3.5. *For any scheme S, E an elliptic curve over S, and $P \in E(S)$ such that $P, 2P, 3P \neq 0$ on any fibre, there exists unique $\alpha, \beta \in \Gamma(S, \mathcal{O}_S)$ such that $\Delta(\alpha, \beta) \in \Gamma(S, \mathcal{O}_S)^*$ and a unique isomorphism $E(\alpha, \beta) \xrightarrow{\sim} E$ mapping $(0, 0)$ to P.*

Proof. First, assume E has a Weierstrass equation over S. By a translation $x \mapsto x + s$, $y \mapsto y + t$ we can assume $P = (0, 0)$. Since P does not have order 2 in any fibre, the gradient of tangent line at P is in $\Gamma(S, \mathcal{O}_S)$, so by replacing y with $y + rx$ for some r we can put equations in the form $Y^2 + a_1XY + a_3Y = X^3 + a_2X^2$, with $a_i \in \Gamma(S, \mathcal{O}_S)$.

Since P does not have order 3 in any fibre, $(0, 0)$ is not an inflexion point, so $a_2 \in \Gamma(S, \mathcal{O}_S)^*$. So by scaling $x \mapsto u^2x$ and $y \mapsto u^3y$, we have that $a_2 = a_3$. Then E is $E(\alpha, \beta)$ where $\alpha = a_1, \beta = a_2$.

This gives an isomorphism to a curve in Tate normal form.

Now consider a general E over S. We know there exists an affine covering $S = \cup_i U_i$ such that $E|_{U_i}$ has a Weierstrass equation over $\Gamma(U_i, \mathcal{O}_S)$. So we get $\alpha_i, \beta_i \in \Gamma(U_i, \mathcal{O}_S)$ such that $(E|_{U_i}, P|_{U_i}) \cong (E(\alpha_i, \beta_i), (0, 0))$. Since α_i, β_i are unique, they must agree on $U_i \cap U_j$. By the sheaf property of $\mathcal{O}_S$, we have that there exists $\alpha, \beta \in \Gamma(S, \mathcal{O}_S)$ such that $\mathrm{res}_{U_i}(\alpha) = \alpha_i$ and $\mathrm{res}_{U_j}(\beta) = \beta$ for all i. Then $(E, P) \cong (E(\alpha, \beta), (0, 0))$. □

Remark. The last step used in an essential way the uniqueness of (α, β): "local uniqueness give global existence".

Corollary 3.6.

1. *The pair* $(\operatorname{Spec} \mathbb{Z}[A, b, \Delta(A, B)^{-1}], (E(A, B), (0, 0))$ *represent the functor* $\underline{\mathrm{Sch}}^{\mathrm{opp}} \to \underline{\mathrm{Set}}$ *defined by* $S \mapsto \{(E, P) | E/S$ elliptic c
2. *The pair* $(\operatorname{Spec} \mathbb{Z}[B, \Delta(1+B, B)^{-1}], (E(1+B, B), (0, 0)))$ *represents* $S \mapsto \{(E, P) \big| E/S$ elliptic curve and P point of exact orde

Proof.

1. This is a restatement of Proposition 3.5
2. Just equate $3P = -2P$. We have $3P = (1 - A, A - B - 1)$ and $-2P = (-B, 0)$.

□

Note. $\Delta(1 + B, B) = B^5(B^2 + 11B - 1)$. The discriminant of the quadratic is 5^3.

Is it reasonable to define "$Y_1(5)_\mathbb{Z}$" to be $\operatorname{Spec} \mathbb{Z}[B, \Delta(1 + B, B)^{-1}]$. Sadly no: our definition of "point of exact order 5" is too naive in characteristic 5. If E over $\mathbb{F}_5$ is supersingular, $E[5]$ is a single point with multiplicity 25. So there are no points of order 5, even over $\overline{\mathbb{F}}_5$. So this scheme $\operatorname{Spec} \mathbb{Z}[B, \Delta(1 + B, B)^{-1}]$ has empty fibre over supersingular j-invariants.

Definition 3.7. We set $Y_1(5)_{\mathbb{Z}[\frac{1}{5}]} = \operatorname{Spec} \mathbb{Z}\left[\frac{1}{5}, B, \Delta(1+B,B)^{-1}\right]$, and this represents the same functor as before on category of $\mathbb{Z}\left[\frac{1}{5}\right]$-schemes

More generally: For $N \geq 4$, let $\mathcal{Y}_N$ = closed subscheme of $\mathcal{Y} = \operatorname{Spec} \mathbb{Z}[A, B, \Delta(A,B)^{-1}]$, where $N \cdot (0,0,1) = (0,1,0)$, and let

$$Y_1(N)_{\mathbb{Z}\left[\frac{1}{N}\right]} = \left(\mathcal{Y}_N - \bigcup_{d|N, 4 \leq d < N} \mathcal{Y}_d\right) \times_{\operatorname{Spec} \mathbb{Z}} \operatorname{Spec} \mathbb{Z}\left[\frac{1}{N}\right]$$

By construction this represents $S \mapsto$ (elliptic curve E/S with point of exact order N) on the category of $\mathbb{Z}[\frac{1}{N}]$-schemes. (More precisely, $Y_1(N)_{\mathbb{Z}\left[\frac{1}{N}\right]}$ has a universal elliptic curve over it by restricting $E(A,B)/\mathcal{Y}$, and this has a point $(0,0)$ and $(Y_1(N)_{\mathbb{Z}\left[\frac{1}{N}\right]}, (\text{this curve, this point}))$ represents the above functor)

Two natural questions:

1. What does $Y_1(N)_{\mathbb{Z}\left[\frac{1}{N}\right]}$ look like? Is it non-singular?
2. There exists a bijection of sets between $Y_1(N)_{\mathbb{Z}\left[\frac{1}{N}\right]}(\mathbb{C})$ and $\Gamma_1(N)\backslash\mathcal{H}$. Is this a map of algebraic varieties over $\mathbb{C}$?

3.4 Smoothness

Definition 3.8. A morphism of schemes $\phi : X \to Y$ is *smooth* if it's locally of finite presentation, flat, and for every point $y \in Y$, the fibre $\phi^{-1}(y)$ is a smooth variety over $k(y)$.

So our definitions of elliptic curves over S required that $\mathcal{E} \to S$ be a smooth morphism.

Lemma 3.9.

1. *The composition of smooth morphism is smooth*
2. *If E over S is an elliptic curve and $N \geq 1$ is invertible on S, then $[N] : E \to E$ is smooth.*

Proof.

1. is standard (see EGA, follow trail of references from Wikipedia)
2. The morphism $[N]$ multiplies a global differential by N, so it induces an isomorphism on tangent space, i.e., it's on étale morphism. (and étale morphism are smooth)

□

Proposition 3.10 (Functorial criterion for smoothness)**.** *Let $X \to \operatorname{Spec} R$ be a scheme of finite type over R, with R Noetherian. The map $X \to \operatorname{Spec} R$ is a smooth morphism if and only if it's "formally smooth", i.e., for every local R-algebra A and nilpotent ideal $I \subset A$, the map $\operatorname{Hom}_{\text{Scheme}/R}(\operatorname{Spec} A, X) \to \operatorname{Hom}_{\text{Scheme}/R}(\operatorname{Spec} A_0, X)$ is surjective, where $A_0 = A/I$.*

If we replace surjective with bijective, we get a notion of formally étale

Proof. See Stacks Project, section 36.9 □

Theorem 3.11. *$Y_1(N)_{\mathbb{Z}\left[\frac{1}{N}\right]}$ is smooth over $\mathbb{Z}\left[\frac{1}{N}\right]$.*

Proof. Let A be a local $\mathbb{Z}\left[\frac{1}{N}\right]$-algebra, $I \subset A$ nilpotent. Let $(E_0, P_0) \in Y_1(N)(A_0)$. Since A_0 is local, we have E_0 has a Weierstrass equation over $\operatorname{Spec}(A_0)$. Lift coefficients arbitrarily to A to get an E/A lifting of E_0. (The discriminant $\Delta(E)$ is in A^* as its image in A_0 is in A_0^*). Can we lift P_0 to an N-torsion point on E? In other words, is $E[N]$ smooth? But it is, because $[N] : E \to E$ is smooth and a composition of smooth morphism is smooth. ($[N]$ composed with the structure map $E \to \operatorname{Spec} A$). So (E_0, P_0) lifts to (E, P) and we are done. □

Note. The schemes $\mathcal{Y}_N$ over $\mathbb{Z}$ are very rarely smooth, this was true for $N = 5$ essentially by accident.

3.5 A complex - analytic digression

Let $\Lambda \subset \mathbb{C}$ be a lattice.

Definition 3.12. The Weierstrass $\wp$-function $\wp_n(z)$ is the unique holomorphic function $\mathbb{C}/\Lambda \to \mathbb{P}^1(\mathbb{C})$ such that $\wp_n(z) = \frac{1}{z^2} + \mathcal{O}(1)$ at $z = 0$, and $\wp_n(z)$ is holomorphic away from Λ. (The x-coordinate correspond to differential dz)

The machinery of Proposition 3.3 implies that $\mathbb{C}/\Lambda$ is isomorphic to $Y^2 = X^3 - g_4X - g_6$ via $z \mapsto (\wp(z), -\frac{1}{2}\wp'(z))$, where g_4 and g_6 are constants depending on Λ.

If $\Lambda = \Lambda_\tau := \mathbb{Z} + \mathbb{Z}\tau$, then g_4 and g_6 are constant multiples of Eisenstein series E_4, E_6 respectively. Hence they are holomorphic functions of τ.

Proposition 3.13. *Let $\mathcal{U} = \{(\tau, z) \in \mathcal{H} \times \mathbb{C} : z, 2z, 3z \notin \Lambda_\tau\}$. Then there exists a holomorphic map $U \overset{(\alpha,\beta)}{\to} \mathbb{C}^2 \setminus \{\alpha, \beta | \Delta(\alpha, \beta) = 0\}$ such that $E(\alpha(\tau, z), \beta(\tau, z)) \cong \mathbb{C}/\Lambda_\tau$ and $(0, 0) \leftarrow z \mod \Lambda_\tau$.*

Proof. Start from the pair $(Y^2 = X^3 - g_4X - g_6, (\wp(z), -\frac{1}{2}\wp'(z)))$ (with g_4, g_6 correspond to Λ_τ), manipulate as in Proposition 3.5 to put this in Tate normal form. All coefficients of rescaling and translations are holomorphic on U as functions of (τ, z). Hence so are the resulting α, β. □

Corollary 3.14. *$Y_1(N)_{\mathbb{Z}[\frac{1}{N}]}(\mathbb{C})$ is isomorphic as a Riemann surface to $\Gamma_1(N)\backslash\mathcal{H}$.*

Recall: We characterized $Y_0(N)$ over $\mathbb{Q}$ using q-expansions.

Proposition 3.15 (Siegel, Kato 2004)**.** *Let E be an elliptic curve over S, $c > 1$ an integer not divisible by 2 or 3. There exists a unique element ${}_c\theta_E \in \mathcal{O}(E \setminus E[c])^*$ with the following properties:*

1. $\mathrm{div}({}_c\theta_E) = c^2 \cdot (0) - E[c]$
2. *$N_a({}_c\theta_E) = {}_c\theta_E$ for a coprime to c, where N_a is the norm map $\mathcal{O}(E \setminus E[ac])^* \to \mathcal{O}(E \setminus E[c])^*$ attached to the a-multiplication on E.*

Moreover, if $E = \mathbb{C}/(\mathbb{Z} + \mathbb{Z}\tau)$, $S = \mathbb{C}$, we have ${}_c\theta_E = q^{\frac{c^2-1}{12}}(-t)^{-c(c-1)/2}\gamma_q(t)^{c^2}\gamma_q(t^c)^{-1}$ where $t = e^{2\pi iz}$ (for $z \in \mathbb{C}/(\mathbb{Z} + \mathbb{Z}\tau)$, $q = e^{2\pi i\tau}$ and $\gamma_q(t) = \prod_{n\geq 0}(1 - q^n t)\prod_{n\geq 1}(1 - q^n t^{-1})$.

Proof. First, note that this unit is unique if it exists. Assume some f satisfying 1. and 2. exits. Any other g satisfying 1. and 2. is $g = uf$ for some $u \in \mathcal{O}(S)^*$. Now $N_3(g) = g$, then $N_3(uf) = uf$, so $u^{3^2}f = uf$, i.e., $u^8 = 1$. Similarly $N_2(g) = g$ implies $u^3 = 1$. Now $u = (u^3)^2(u^8)^{-1} = 1$. Hence we get uniqueness.

It suffices to show that $c^2(0) - E[c]$ is locally on S a prime divisor. There exists a theory of "relative Cartier Divisor" and a map $(\deg 0 \text{ divisor on } E)/(\text{pullback of ones on } S) \to E(S)$. Since $c^2(0) - E[c] = 0$ in $E(S)$. Hence $c^2(0) - E[c]$ is the pullback of a divisor on S, hence locally on S principal.

Let f be such that $\mathrm{div}(f) = c^2(0) - E[c]$. Since $\mathrm{div}(f)$ is invertible under N_a, we must have $N_a(f) = u_a f$ for some $u_a \in \mathcal{O}(S)^*$. Since $N_aN_b = N_bN_a$, $u_a^{(b^2-1)} = u_b^{(a^2-1)}$ for all a, b coprime to c. So if we put $g = u_2^{-3}u_3 f$, we have

$$\begin{aligned} N_a(g) &= u_2^{-3a^2}u_3^{a^2}u_a f \\ &= u_2^{-3(a^2-1)}u_3^{(a^2-1)}u_a g \\ &= u_a^{-3(2^2-1)}u_a^{(3^2-1)}u_a g \\ &= u_a^0 g \\ &= g. \end{aligned}$$

So ${}_c\theta_E$ exists locally and by uniqueness it exists globally.

For the case $S = \mathbb{C}$ and $E = E_\tau$,we just check that the given function has properties 1. and 2. (c.f. the 3rd problem sheet) □

Definition 3.16. For $N \geq 4$ and $c > 1$ with $\gcd(c, 6N) = 1$, the *Siegel unit* ${}_cg_N$ is the pullback of ${}_c\theta_{\mathcal{E}}$ along the order N section $Y_1(N) \to \mathcal{E}$, where $\mathcal{E}/Y_1(N)$ is the universal elliptic curve.

Remark. These units are the building blocks of Euler systems. (c.f. Kato's paper (Asterisque 295,2004), and Loefler's paper with Lei and Zerbes, 2013)

Important Corollary. *$Y_1(N)$ is not characterised over $\mathbb{Q}$ by having q-expansions of elements of $\mathbb{Q}(Y_1(N))$ in $\mathbb{Q}((q))$.*

Proof. Calculate q-expansions of ${}_cg_5 \in \mathbb{Q}(Y_1(5))^*$. The order N sections is $z = \frac{1}{5} \mod \mathbb{Z} + \mathbb{Z}\tau$, so $t = e^{2\pi i z} = e^{2\pi i/5} \notin \mathbb{Q}$, ${}_cg_5 = q^{(c^2-1)/12}(-e^{2\pi i/5})^{-c(c-1)/2} \prod(\dots)$, which has ζ_5's everywhere. □

One can show: $f \in \mathbb{Q}(Y_1(N))$ if and only if $f \in \mathbb{C}(Y_1(N))$ and its q-expansion lands in $\mathbb{Q}(\zeta_N)((q))$ and satisfies $a_n(f)^\sigma = a_n(\langle\sigma\rangle f)$ for all $\sigma \in \mathrm{Gal}(\mathbb{Q}(\mu_N)/\mathbb{Q}) \cong (\mathbb{Z}/N)^*$.

3.6 Quotients and $Y_0(N)$

Proposition 3.17. *Let X be a quasi-projective S-scheme (for some base scheme S) and G a finite group action on X by S-automorphisms. Then there exists a unique S-scheme X/G and a morphism $X \to X/G$ representing the functor $Y \mapsto$ (homomorphism of S shcemes $X \to Y$ commuting with $G-$actions).*

Proof. Uniqueness is obvious (representing a functor). So we prove existence: for $X = \mathrm{Spec}(A)$ affine, then $\mathrm{Spec}(A^G)$ works; and can show these patches nicely. (we need quasi-projectivity and finiteness of G here) □

Definition 3.18. For $N \geq 4$ let $Y_0(N) = Y_1(N)/(\mathbb{Z}/N\mathbb{Z})^*$. (as a $\mathbb{Z}\left[\frac{1}{N}\right]$-scheme).

The $\mathbb{C}$-points of this are $\Gamma_0(N)\backslash\mathcal{H}$.

Construction

Let S be a $\mathbb{Z}\left[\frac{1}{N}\right]$-scheme. There is a map

$$\begin{aligned}&\{\text{isomorphism classes of pairs } (E, C)\}\\ &\{E/S \text{ elliptic curve}, C \subset E \text{ subgroups} - \text{scheme}\} \to Y_0(N)(S)\\ &\{\text{étale locally isomorphic to } \mathbb{Z}/N\mathbb{Z}\}\end{aligned}$$

defined as follows: Let (E, C) be in the LHS; then there exists $S' \to S$ étale and $P \in E(S')$ such that $C = \langle P\rangle$, and this gives a point of $Y_1(N)(S')$. Channing P changes this by an element of $G = (\mathbb{Z}/N\mathbb{Z})^*$. So we get a G-orbit of elements of $Y_1(N)(S')$. By a scar lemma ("étale descent of morphism") this gives an S-point of $Y_0(N)$. Thus we have a well-defined map $L_S : \{(E, C)/S\} \to Y_0(N)(S)$. In general this is neither injective nor surjective, but if S is $\mathrm{Spec}(\overline{k})$ for some $\overline{k}$ algebraic closed, it's a bijection.

Injectivity: If L/K is a finite field extension $Y_0(N)(K) \to Y_0(N)(L)$ is obviously injective, but $((E, C)/K) \to ((E, C)/L)$ is not injective (there exists obsturctions coming from quadratic twists, etc). For a field k, we can check that the image (L_k) is the set of pairs (E, C) defined over k modulo isomorphism over $\overline{k}$.

Surjectivity: We can show that for a field k, L_k is surjective (fairly hard, c.f. Proposition VI.3.2 of Deligne - Rapopok) but for non-field S surjectivity can also fail. For instance, $S = Y_0(N)$ itself; in general there is no (E, C) which correspond to the identity map. (Can try to use $E/(\mathbb{Z}/N\mathbb{Z})^*$ but fibres over points of $Y_0(N)$ with nontrivial stabilizers might not be elliptic curves!).

Fact. *$Y_0(N)$ is smooth over $\mathbb{Z}\left[\frac{1}{N}\right]$, and it agrees with our earlier construction over $\mathbb{Q}$. (Sketch of last point, it suffices to show $j(z)$ and $j(Nz)$ lies in $\mathbb{Q}(Y_1(N))^G$, just take $j(E)$ and $j(E/\langle P\rangle)$.)*

3.7 General Modular Curves

This section is following Katz - Mazur.

Definition 3.19. Let R be a ring:

1. Let $\underline{\mathrm{Ell}/R}$ be the following category:
   - Objects are diagrams $E \to S$ where S is some R-scheme and E is an elliptic curve
   - Morphisms are squares
   $$\begin{array}{ccc} E & \longrightarrow & E' \\ \downarrow & & \downarrow \\ S & \longrightarrow & T \end{array}$$
   where $E \cong E' \times_T S$.
2. A *moduli problem for elliptic curves over* R is a contravariant functor $\mathcal{P} : \underline{\mathrm{Ell}/S} \to \underline{\mathrm{Set}}$.
3. We say that $\mathcal{P}$ is:
   - *representable* if it is representable.
   - *relatively representable* if, for every $E/S \in \mathrm{Obj}(\underline{\mathrm{Ell}/R})$, the functor $\underline{\mathrm{Sch}/S} \to \underline{\mathrm{Sets}}$ defined by $T \mapsto \mathcal{P}(E \times_S T/T)$ is representable.

Aside: The category $\underline{\mathrm{Ell}/R}$ is "$\underline{\mathrm{Sch}/Y}$ for a Y that doesn't exists". If functor $S \mapsto \{\mathrm{ell-curve}/S\}$ were representable, by some $(Y, E/Y)$, then objects of $\underline{\mathrm{Ell}/R}$ would be maps $S \to Y$. This is the idea of $\underline{\mathrm{stacks}}$.

Proposition 3.20. *For $\mathcal{P}$ a moduli problem let $\widetilde{\mathcal{P}} : \underline{\mathrm{Sch}/R} \to \underline{\mathrm{Sets}}$ be defined by $S \mapsto (\mathrm{pairs}\,(E, \alpha),\ E/S\,\mathrm{ell\,curve}, \alpha \in \mathcal{P}(E, S))$. If $\mathcal{P}$ is representable on $\underline{\mathrm{Ell}/R}$, then $\widetilde{P}$ is representable on $\underline{\mathrm{Sch}/R}$.*
(The converse is not quite true).

Proof. If $(E/S, \alpha)$ represents $\mathcal{P}$, can check $(S, (E, \alpha))$ represents $\widetilde{\mathcal{P}}$. □

Definition 3.21. $\mathcal{P}$ is *rigid* if for all all $E/S \in \mathrm{Obj}(\underline{\mathrm{Ell}/R})$, $\mathrm{Aut}(E/S)$ acts on $\mathcal{P}(E/S)$ without fixed points.

Exercise.

1. A representable functor is rigid.
2. If $\mathcal{P}$ is rigid and $\widetilde{\mathcal{P}}$ is representable, then $\mathcal{P}$ is representable.

Theorem 3.22 (Katz - Mazur)**.** *$\mathcal{P}$ is representable if and only if it is relatively representable and rigid.*

Sketch of Proof. Start from 2 basic moduli problems:

- "naive level $\Gamma(3)$" over $\mathbb{Z}\left[\frac{1}{3}\right]$.
- "Legendre moduli problem" ($\Gamma(2)$ and choice of differential) over $\mathbb{Z}\left[\frac{1}{2}\right]$.

Both have group action ($\mathrm{GL}_2(\mathbb{F}_3)$ and $\mathrm{GL}_2(\mathbb{F}_2) \times \{\pm 1\}$). Given $\mathcal{P}$ is relatively representable and rigid, construct one object by taking $\mathcal{E}/Y(3)$ - relative representability gives us a scheme over $Y(3)$ and this has a $\mathrm{GL}_2(\mathbb{F}_3)$ action. Take inverse (this is fine since $\mathcal{P}$ is rigid), and this gives an object $\mathcal{E}/S$ representing $\mathcal{P}$ on $\mathrm{Ell}/R[\frac{1}{3}]$. Legendre gives an object over $R[\frac{1}{2}]$ similarly. By rigidity these agree over $R\left[\frac{1}{6}\right]$, so we get a representing object over R. □

3.8 General Level Structure

Fix N and a subgroup $H \subset \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$.

Fact 3.23. *There exists a moduli problem $\mathcal{P}_H$ on $\mathrm{Ell}/\mathbb{Z}\left[\frac{1}{N}\right]$ such that if $\overline{k}$ is algebraic closed, $E/\overline{k} \in \mathrm{Obj}\left(\mathrm{Ell}/\mathbb{Z}\left[\frac{1}{N}\right]\right)$:*

$$\mathcal{P}_H(E/\overline{k}) = \left\{H-\text{orbits of isomorphisms } (\mathbb{Z}/\mathbb{Z}N)^2 \xrightarrow{\sim} E[N]\right\}.$$

For $H = \left\{\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\right\}$, this is $\Gamma(N)$, $E/S \mapsto$ (pairs of sections $P, Q \in E[S]$ generating $E[N]$ in every fibre).

For $H = \left\{\begin{pmatrix}* & *\\ 0 & 1\end{pmatrix}\right\}$, this is the $\Gamma_1(N)$.

For $H = \left\{\begin{pmatrix}* & *\\ 0 & *\end{pmatrix}\right\}$, it's $\Gamma_0(N)$.

Remark. If k is a field, E/k, then the image of $\mathcal{P}_H(E/k)$ in $\mathcal{P}_H(E/\overline{k})$ is $\left\{H-\text{orbit of bases of } E[N]\left(\overline{k}\right) \text{ in which image of } \mathrm{Gal}(\overline{k}/k) \text{ la}\right.$

Proposition 3.24. *$\mathcal{P}_H$ is relative representable and "étale over $\mathrm{Ell}/\mathbb{Z}\left[\frac{1}{N}\right]$". (This means: for all $E/S \in \mathrm{Obj}(\mathrm{Ell}/\mathbb{Z}\left[\frac{1}{N}\right])$, the functor $T \mapsto \mathcal{P}_H(E \times_S T)$ is represented by an étale S-scheme.)*

Proof. For $H = \{1\}$, for $E/S \in \mathrm{Obj}(\mathrm{Ell}/\mathbb{Z}\left[\frac{1}{N}\right])$, we can find an explicit S-scheme representing $\mathcal{P}_H$ on Schemes over S. It's an open subscheme of $E[N] \times_S E[N]$ given by non-vanishing of Weil pairing.

For general H just take the quotient of this by H. □

So it is easier to relatively represent $\mathcal{P}_H$ than it is to define it.

Proposition 3.25. *$\mathcal{P}_H$ is rigid on $\mathrm{Ell}/R\left[\frac{1}{6}\right]$ if and only if the preimage in $\mathrm{SL}_2(\mathbb{Z})$ of $H \cap \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ contains no elements of finite order (i.e., has no elliptic points and does not contain -1).*

Sketch of Proof. Over $\mathbb{C}$ this is routine. To prove general statement it suffices to check it on objects $E/\overline{k}$, where $\overline{k}$ is algebraic closed. If $\overline{k}$ has characteristic 0, we can embed it into $\mathbb{C}$.

We can show that, if k has finite characteristic ≥ 5, E/k an elliptic curve and $\phi \in \mathrm{Aut}(E)$, then the pair (E, ϕ) lifts to characteristic 0. (c.f. somewhere in chapter VI of Deligne - Rapoport) □

This gives a complete classification of modular curves and their associated moduli problems.

Remark.

1. As in the case of $Y_0(N)$ for H non-rigid, we can still construct a $\mathbb{Z}\left[\frac{1}{N}\right]$-scheme which is "the best approximation" to representing $\widetilde{\mathcal{P}}_H$; we have a map $\widetilde{\mathcal{P}}_H(S) \to Y(S)$, which is surjective for S a field, and a bijection if for S algebraic closed.

2. If $\Gamma = \mathrm{preimage}(H) \subset \mathrm{SL}_2(\mathbb{Z})$, then $Y_{\mathcal{P}_H}(\mathbb{C})$ is not quite $\Gamma\backslash\mathcal{H}$. It's a union of such things corresponding to quotient $(\mathbb{Z}/N\mathbb{Z})^*/\det H$. In particular, our version of $Y(N)$ is not geometrically connected. We can write $Y_{\mathcal{P}_H}(\mathbb{C})$ more intrinsically as $\mathrm{GL}_2(\mathbb{Q})\backslash\mathrm{GL}_2(\mathbb{A})/(\mathbb{R}_{>0} \cdot \mathrm{SO}_2(\mathbb{R}) \cdot U)$ where $U = \mathrm{preimage}(H) \subset \mathrm{GL}_2(\widehat{\mathbb{Z}}) \subset \mathrm{GL}_2(\mathbb{A}_{\mathrm{fin}})$.

4 Leftovers

4.1 Katz Modular Forms

Recall we defined, for E an elliptic curve over S,$\omega_{E/S} = \pi_*(\Omega^1_{E/S})$.

Proposition 4.1. *If $S = Y_{\mathcal{P}_H}$ for some H as before, E/S universal elliptic curve, then $\omega_{E/S}$ is the "Katz Sheaf" from Chapter 2.*

Proof. Just unravel the definitions. We will show that both have the same pullback to $\mathcal{H}$ and the actions of Γ agree.

By definition, the pullback of ω_{Katz} is $\mathbb{C}$. The pullback of $\omega_{E/S}$ is π_*(relative differentials on $\mathbb{C}/(\mathbb{Z}+\tau\mathbb{Z})) = \mathbb{C}\cdot(2\pi i dz)$. But the isomorphism $\mathbb{C}/(\mathbb{Z}+\mathbb{Z}\tau) \cong \mathbb{C}/(\mathbb{Z}+\gamma\tau\mathbb{Z})$ for $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ is multiplication by $(c\tau+d)^{-1}$ on $\mathbb{C}$, so it multiplies dz by this constant. So the action coincides with the one we defined in the construction of ω_{Katz}. □

Definition 4.2. For Γ a torsion free congruent subgroup of level N, R a $\mathbb{Z}\left[\frac{1}{N}\right]$-algebra, we define $KM_K(\Gamma, R) = H^0(Y(\Gamma)\times R, \omega^k_{E/Y(\Gamma)\times R})$. (This is an R-module).

Concretely: A Katz Modular form of weight k over R is a rule attaching to each triple $(E/S, \alpha, \omega)$ - where S is a R-scheme, E/S an elliptic curve, $\alpha \in \mathcal{P}_H(E/S)$, ω a basis of $\Gamma(E, \Omega^1_{E/S})$ - an element of $\Gamma(S, \mathcal{O}_S)$ such that

- compatible with base change in S
- Homogeneous of weight k in ω.

(C.f. Katz "P-adic properties of modular schemes and modular forms", Springer LNM #330).

Fun thing: Over $R = \mathbb{Z}\left[\frac{1}{6}\right]$, for any elliptic curve E/R and $\omega \in \Omega^1$, there exists a unique short Weierstrass equation such that $\omega = \frac{dx}{y}$, and E_4 (respectively E_6) are the maps $(E,\omega) \mapsto a_4$ coefficient of this equation (respectively a_6).

4.2 Cups and the Tate curve

Consider the ring $\mathbb{Z}((q)) = \left\{\sum_{n=-N}^{\infty} a_n q^n | a_n \in \mathbb{Z}\right\}$. We'll define an elliptic curve over this and a differential, such that evaluating at this pair gives q-expansion of a Katz MF.

Definition 4.3. Tate(q) = the elliptic curve $y^2 + axy = x^3 + a_4 x + a_6$ where $a_4 = -\sum_{n\geq 1} \frac{5n^3 q^n}{1-q^n}$ and $a_6 = -\sum_{n\geq 1} \frac{(7n^5+5n^3)/12\cdot q^n}{1-q^n}$. (Note $a_4, a_6 \in \mathbb{Z}[[q]]$). The discriminant of this curve is exactly the q-expansion of Δ(weight 12 cusp form) in $q + q^2\mathbb{Z}[[q]] \subset \mathbb{Z}((q))^*$.

Hence Tate(q) is an elliptic curve. Tate(q) is "the q-expansion of $\mathbb{C}/(\mathbb{Z}+\tau\mathbb{Z})$" = "$\mathbb{C}^*/q^{\mathbb{Z}}$".

Proposition 4.4. *If $\tau \in \mathcal{H}$, then series defining* Tate(q) *converge at $q = e^{2\pi i\tau}$ and define a curve isomorphic to $\mathbb{C}/(\mathbb{Z}+\tau\mathbb{Z})$.*

Convergence is easy, and we check if $j(\text{Tate}(q))$ is the q-expansion of $j(\tau)$.

Proposition 4.5. *Let $\oplus$ denote the group law on* Tate(q). *There exists series $X(u,q), Y(u,q) \in \mathbb{Z}\left[u, u^{-1}, (1-u)^{-1}\right][[q]]$ such that $(X(u,q), Y(u,q)) \oplus (X(v,q), Y(v,q)) = (X(uv,q), Y(uv,q))$. (Interpret $X(u,q), Y(u,q)$ as ∞ if $u = 1$).*

Proof. Take

$$\begin{aligned} X(u,q) &= \frac{u}{(1-u)^2} + \sum_{d\geq 1}\left(\sum_{m|d} m(u^m + u^{-m} - 2)\right) q^d \\ Y(u,q) &= \frac{u^2}{(1-u)^3} + \sum_{d\geq 1}\left(\sum_{m|d}\left\{\frac{m(m-1)}{2}u^m - \frac{m(m+1)}{2}u^{-m} + m\right\}\right) q^d. \end{aligned}$$

Sneaky part, there exists a straightforward change of coordinates from Tate(q) to $y^2 = 4x^3 - g_4(\tau)x - g_6(\tau)$, which is $\mathbb{C}/(\mathbb{Z} + \tau\mathbb{Z})$ via $(\wp(z,\tau), \wp'(z,\tau))$. Then X and Y are just $\wp$ and $\wp'$ as power series in $u = e^{2\pi i z}$, $q = e^{2\pi i \tau}$.

So the identity $(X(u,q), Y(u,q)) \oplus (X(v,q), Y(v,q)) = (X(uv,q), Y(uv,q))$ holds for all u, q in an open subset of $\mathbb{C} \times \mathbb{C}$, so it holds as an identity of power series. □

Proposition 4.6. *Cusps of* $Y_{\mathcal{P}_H} \leftrightarrow \{\mathcal{P}_H$ *level structures on* Tate(q) *over* $\mathbb{Z}[[q^{\frac{1}{N}}, \zeta_N]]$, *modulo automorphism* $q^{\frac{1}{N}} \mapsto \zeta_N^a q^{\pm\frac{1}{N}}\}$.

And we thus get an action of Gal$(\mathbb{Q}(\mu_N)/\mathbb{Q})$.

Example. $Y_1(5)$.

Points of order 5 on Tate(q) over $\mathbb{Z}\left[\frac{1}{5}, \zeta_5\right][[q^{\frac{1}{5}}]]$ are (images of) $q^{a/N}\zeta_n^b$, where $a, b \in (\mathbb{Z}/5\mathbb{Z})^2 \setminus \{(0,0)\}$.