Recall .0.1

$\mathbb{C}(X(N))/\mathbb{C}(X(1))$ is Galois with group $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\pm I$.

How to check? We have a map $\theta : \mathrm{SL}_2(\mathbb{Z}) \to \mathrm{Aut}(\mathbb{C}(X(N)))$ via $\mathrm{SL}_2(\mathbb{Z})$ acting via conjugation on $\Gamma(N)$ (giving us $\mathrm{SL}_2(\mathbb{Z})$ acting on functions). This is our hammer, and we've used it before (recall $f[\alpha]$).

It is easy to check that $\ker\theta = \pm I \cdot \Gamma(N)$. Then $\ker\theta = \pm I\Gamma(N)$. Then $\theta(\mathrm{SL}_2(\mathbb{Z}))$ in fact fixes $\mathbb{C}(X(1))$. Thus this gives a map into the Automorphism group. By Galois Theory, the fixed field will be some field extension, and it is not hard to show the fixed field is in fact $\mathbb{C}(X(1))$, which tells us everything we need.

Unrelated Note: If you want to know something about Weil groups, there's stuff from Tate from the Corvallis Conference with a nice note called Number Theory Background.

Recall that for Λ_τ given as $\mathbb{Z}\cdot 1 \oplus \tau\mathbb{Z}$, we have a map

$$\begin{aligned}\mathbb{C}/\Lambda_\tau &\to E_\tau \\ z &\mapsto (\wp_\tau(z), \wp'_\tau(z)),\end{aligned}$$

and the Elliptic Curve is as

$$E_\tau : y^2 = 4x^3 - g_2(\tau)x - g_3(\tau).$$

Recall that $f_0^{\overline{v}} = \frac{g_2(\tau)}{g_3(\tau)}\wp_\tau\left(\frac{cv\tau+dv}{N}\right)$. One should think of this is the X-coordinate of some N-torsion

Suppose $j(\tau) \notin \{0, 1728\}$. This implies that $g_2(\tau), g_3(\tau)$. We then define

$$\begin{aligned}\mathbb{C}/\Lambda_\tau &\to \mathbb{C}^2 \cup \{\infty\} \\ z &\mapsto \left(\frac{g_2(\tau)}{g_3(\tau)}\wp_\tau, \left(\frac{g_2(\tau)}{g_3(\tau)}\right)^{3/2}\rho'_\tau\right)\end{aligned}$$

this takes the torus to another elliptic curve $Ej(\tau)$ with equation

$$Ej(\tau) : y^2 = 4x^3 - \frac{(g_2(\tau))^3}{(g_3(\tau))^2}x - \frac{(g_2(\tau))^3}{(g_3(\tau))^2}.$$

This is an admissible change of variables from E_τ. Now $f_0^{\overline{v}}$ are x-coordinates of $E_{j(\tau)}[N]$. Moreover, if we let $v = (1,0), (0,1)$, this gives points P_τ, Q_τ which are a basis for the N-torsion.

We can rewrite the equations as

$$E_j : y^2 = 4x^3 - \left(\frac{27j}{j-1728}\right)x - \left(\frac{27j}{j-1728}\right).$$

We'll call this a "universal elliptic curve" over $X(1)$. There are two ways to think about this. We could say it's an ellitpic curve over $\mathbb{C}(X(1)) = \mathbb{C}(j)$, or we can think of it as

$$\begin{array}{ccc} E_c & \longrightarrow & E_j \\ \downarrow & & \downarrow \\ \mathrm{Spec}\,\mathbb{C} & \xrightarrow[c]{} & X(1)_{\mathrm{alg}} \end{array}$$

where we view $X(1)_{\mathrm{alg}}$ as the algebraic curve with function field $\mathbb{C}(X(1))$. We can enhance this elliptic curve as (E_j, P_τ, Q_τ), and this will live over $X(N)$.

Digression: There will be some functor $\mathcal{M}$: Schemes $\to$ Sets which is called a "moduli functor." In some sense this is

$$S \mapsto \{\text{"objects" over } S\},$$

where the objects could be interesting (say elliptic curves over S). The functor is called "representable" by some scheme M if

$$\mathcal{M}(S) \simeq \mathrm{Hom}(S, M),$$

with naturality in S. If this is true there's an incredible trick one can do. What if you let $S = M$. Then

$$\mathcal{M}(M) = \mathrm{Hom}(M, M).$$

This has a canonical element Id_M, which gives a *canonical* object over M. We'll call this $M_{\mathrm{univ}} \to M$. Messing with the Yoneda lemma tells us for any $S \to M$ we have

$$\begin{array}{ccc} S \times_M M_{\mathrm{univ}} & \longrightarrow & M_{\mathrm{univ}} \\ \downarrow & & \downarrow \\ S & \longrightarrow & M. \end{array}$$

This is what is called a "fine moduli space." It turns out $X(1)_{\mathrm{alg}}$ is NOT a "fine moduli space." There's some issue with it really being a compactification of $Y(1)$.

But even worse, we've thrown out $0, 1728$, which are the elliptic points. So our universal elliptic curve is just a close approximation of this.

Then $\mathbb{C}(X(N)) = \mathbb{C}(j, X(E_j[N]))$ over $\mathbb{C}(j)$. We can also adjoin the y-coordinates

$$\left(\frac{g_2(\tau)}{g_3(\tau)}\right)^{3/2} \wp'_\tau\left(\frac{c_v\tau + d_v}{N}\right).$$

One can show the Galois group of $\mathbb{C}(j, E_j[N])$ over $\mathbb{C}(j)$ is $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$, making it an extension of $\mathbb{C}(j, X(E_j[N])$.

Now lets look at this over $\mathbb{Q}$. The coefficients of E_j live in $\mathbb{Q}(j)$. Hence we get something like

$$\mathbb{Q}(j) \subseteq \mathbb{Q}(j, E_j[N]),$$

and this is still Galois. But the Galois group will be larger. The key is the roots of unity

$$\mu_N = \{z \in \overline{\mathbb{Q}} \mid z^N = 1\}.$$

We set

$$H_{\mathbb{Q}} = \mathrm{Gal}(\mathbb{Q}(\mu_N, j, E_j[N])/\mathbb{Q}(j)).$$

We have a map $H_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. Where does it come from? Well $H_{\mathbb{Q}}$ acts on $E_j[N] \cong (\mathbb{Z}/N\mathbb{Z})^2 \subseteq \overline{\mathbb{Q}(j)}$.

Lemma .0.1

Take $\sigma \in H_{\mathbb{Q}}$, then for $\mu \in \mu_N$ we have

$$\sigma(\mu) = \mu^{\det(\rho(\sigma))}.$$

Proof. Use results from last time, since the Weil pairing is surjective we win.

Now if $\sigma \in H_{\mathbb{Q}}$ fixes $E_j[N]$ then $\sigma \in \ker(\rho)$, so $\sigma \in \ker(\det(\rho))$, so σ fixes μ_N. This implies $\mu_N \subseteq \mathbb{Q}(j, E_j[N])$. Another way to do this is the Weil pairing has an algebraic formula with coefficients in $\mathbb{Q}(j)$ and is surjective.

And also $\rho_\star = \rho\big|_{H_{\mathbb{Q}(\mu_N)}} : H_{\mathbb{Q}(\mu_N)} \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$, where $H_{\mathbb{Q}(\mu_N)} \subseteq H_{\mathbb{Q}}$ fixes the roots of unity. The original ρ is injective since if you fix $E_j[N]$ then you fix all of $\mathbb{Q}(\mu_N, j, E_j[N]) = \mathbb{Q}(j, E_j[N])$.

But then $\rho_\star$ injects into $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. Well Galois Theory says we can take the situation over complex numbers

$$\begin{array}{ccc} \mathbb{C}(j, E_j[N]) & & \mathbb{Q}(j, E_j[N]) \\ {\scriptstyle \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})}\big| & & \big| \\ \mathbb{C}(j) & & \mathbb{C}(j) \cap \mathbb{Q}(j, E_j[N]) \\ & & \big| \\ & & \mathbb{Q}(j) \end{array} .$$

This implies $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ injects into $H_{\mathbb{Q}(\mu_N)}$. Therefore $H_{\mathbb{Q}(\mu_N)} \cong \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. Thus $H_{\mathbb{Q}} \cong \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, via some basic group theory.

We can then look at Modular Curves as Algebraic Curves. In particular, we have all these function fields

$$\begin{array}{ccc} \mathbb{Q}(j, E_j[N]) & \rightsquigarrow & X(N)_{\mathrm{alg}} \\ \big| & & \big| \\ \mathbb{Q}(j, F_1) & \rightsquigarrow & X_1(N)_{\mathrm{alg}} \\ \big| & & \big| \\ \mathbb{Q}(j, F_0) & \rightsquigarrow & X_0(N)_{\mathrm{alg}} \\ \big| & & \big| \\ \mathbb{Q}(j) & \rightsquigarrow & X(1)_{\mathrm{alg}} \end{array}$$

where $\mathbb{Q}(j, E_j[N])$ is Galois over $\mathbb{Q}(j), \mathbb{Q}(j, F_0), \mathbb{Q}(j, F_1)$. Thus these correspond to projective nonsingular curves. This is what we define as the algebraic version on the right hand side.

This allows us to formula algebraic versions of modularity. $X_0(N)_{\mathrm{alg}} \to E$ and $J_0(N)_{\mathrm{alg}} \to E$ which is a homomorphism.

And as discussed previously if $f \in S_2(\Gamma_0(N))$ then we want to look at a homomorphism $A'_{f,\mathrm{alg}} \to E$.