Goal: Show that geometric moduli space & the analytic modular curve are isomorphic,

What is moduli space & modular curve.

Moduli space: Geometric space whose points represent isomorphism classes of mathematical objects.

Modular Curve: Complex curve (a Riemann Surface) obtained by taking the upper half-plane $\mathbb{H}$ & quotienting by a modular group.

Today's goal is to prove that geometric moduli space $S_1(N)$ and the analytic modular curve $Y_1(N)$ are isomorphic.

$$S_1(N) \cong Y_1(N)$$

The moduli space for $\Gamma_1(N)$ is $S_1(N) = \{[E_\tau, 1/N + \Lambda_\tau] : \tau \in \mathbb{H}\}$

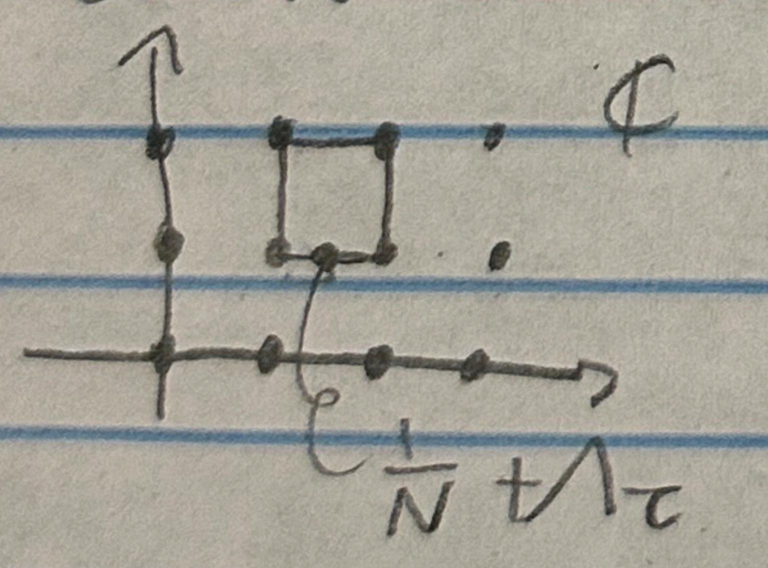
The modular curve for $\Gamma_1(N)$ is $Y_1(N) = \Gamma_1(N) \backslash \mathbb{H}$.

* $E_\tau = \mathbb{C}/\Lambda_\tau$ elliptic curve obtained by taking the complex plane & identifying points that differ by the lattice $\Lambda_\tau = \mathbb{Z}\tau + \mathbb{Z}$

This is like wrapping the complex plane into a torus.

$1/N + \Lambda_\tau$ the point on that elliptic curve represented by the coset of $\frac{1}{N}$ in $\mathbb{C}/\Lambda_\tau$.

Intuition



When you wrap this lattice cell into a torus, that shifted point becomes a single point on the donut surface. $E_\tau, \frac{1}{N} + \Lambda_\tau$

$[E_\tau, \frac{1}{N} + \Lambda_\tau]$ means "the isomorphism class" of the pair consisting of the elliptic curve and the point on it.

Thm 1.5.1 $S_1(N) \cong Y_1(N)$

$[E_\tau, 1/N + \Lambda_\tau]$ & $[E_{\tau'}, 1/N + \Lambda_{\tau'}]$ are equal iff
$\Gamma_1(N)\tau = \Gamma_1(N)\tau'$. Thus there is a bijection
$\psi_1 : S_1(N) \xrightarrow{\sim} Y_1(N)$, $[\mathbb{C}/\Lambda_\tau, 1/N + \Lambda_\tau] \to \Gamma_1(N)\tau$.

In other words each pair $[E, Q]$, where E is an elliptic curve & Q is a point of order N on E, corresponds uniquely to a point $\tau \in \mathbb{H}$ up to the action of $\Gamma_1(N)$.

Proof.

Take any element $[E, Q] \in S_1(N)$. Recall that every elliptic curve E is isomorphic to some $\mathbb{C}/\Lambda_{\tau'}$, $(\tau' \in \mathbb{H})$. So, $E = \mathbb{C}/\Lambda_{\tau'}$.

Now, because Q is a point of exact order N on E, it can be written in the form $Q = \frac{c\tau' + d}{N} + \Lambda_{\tau'}$.

$\hookrightarrow$ point $Q = z + \Lambda_{\tau'}$ has order N iff $Nz \in \Lambda_{\tau'}$ but $Mz \notin \Lambda_{\tau'}$ for $0 < M < N$. $Nz = c\tau' + d$ for some integers c, d

$\hookrightarrow$ because every element of $\Lambda_{\tau'}$ has the form $m\tau' + n$ with

Since every point is a coset $z + \Lambda_{\tau'}$, $Q = z + \Lambda_{\tau'} \Rightarrow Q = \frac{c\tau' + d}{N} + \Lambda_{\tau'}$

Then $\gcd(c, d, N) = 1$ because the order of Q is exactly N.

$\hookrightarrow$ If $\gcd(c, d, N) = g > 1$, then $(c/g, d/g)$ would give a point whose order is N/g. So Q would only have order N/g, not N.

This means there exist integers a, b, k s.t $ad - bc - kN = 1$.

So we can build matrix $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z})$ that reduces modulo N to an element of $SL_2(\mathbb{Z}/N\mathbb{Z})$.

Since the reduction map $SL_2(\mathbb{Z}) \to SL_2(\mathbb{Z}/N\mathbb{Z})$ is surjective, we can take γ to actually be in $SL_2(\mathbb{Z})$

Define $\tau = \gamma(\tau') = \frac{a\tau' + b}{c\tau' + d}$, Let $m = c\tau' + d$ then $m\tau = a\tau' + b$

$m\Lambda_\tau = m(\mathbb{Z}\tau + \mathbb{Z}) = (a\tau' + b)\mathbb{Z} + (c\tau' + d)\mathbb{Z} = \Lambda_{\tau'}$

$m(\frac{1}{N} + \Lambda_\tau) = \frac{c\tau' + d}{N} + \Lambda_{\tau'} = Q$,

Therefore, we have shown $[E, Q] = [\mathbb{C}/\Lambda_\tau, 1/N + \Lambda_\tau]$. where $\tau \in \mathbb{H}$.
every $[E, Q]$ corresponds to some τ.

If two τ gives the same class, they are $\Gamma_1(N)$-equivalent

Now suppose $\tau, \tau' \in \mathbb{H}$ satisfy $\Gamma_1(N)\tau = \Gamma_1(N)\tau'$.

This means $\exists\, \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_1(N)$ s.t $\tau = \gamma(\tau')$.

Since $\gamma \in \Gamma_1(N)$, we know that $c \equiv 0 \pmod N$, $d \equiv 1 \pmod N$

Let $m = c\tau' + d$. Then as before: $m\Lambda_\tau = \Lambda_{\tau'}$, $m(1/N + \Lambda_\tau) = \frac{c\tau' + d}{N} + \Lambda_{\tau'}$

But because $(c, d) \equiv (0, 1) \pmod N$, $m(1/N + \Lambda_\tau) = 1/N + \Lambda_{\tau'}$

Hence $[\mathbb{C}/\Lambda_\tau, 1/N + \Lambda_\tau] = [\mathbb{C}/\Lambda_{\tau'}, 1/N + \Lambda_{\tau'}]$

Now suppose $[\mathbb{C}/\Lambda_\tau, 1/N + \Lambda_\tau] = [\mathbb{C}/\Lambda_{\tau'}, 1/N + \Lambda_{\tau'}]$.

Then $\exists\, m \in \mathbb{C}$ s.t $m\Lambda_\tau = \Lambda_{\tau'}$, $m(1/N + \Lambda_\tau) = 1/N + \Lambda_{\tau'}$

By lemma 1.3.1, there is some $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ s.t $m\tau = a\tau' + b$, $m = c\tau' + d$. That is $m\begin{pmatrix} \tau \\ 1 \end{pmatrix} = \gamma\begin{pmatrix} \tau' \\ 1 \end{pmatrix}$ $m(1/N + \Lambda_\tau) = 1/N + \Lambda_{\tau'}$, then gives $\frac{c\tau' + d}{N} + \Lambda_{\tau'} = \frac{1}{N} + \Lambda_{\tau'}$, Hence $(c, d) \equiv (0, 1) \pmod N$, $\gamma \in \Gamma_1(N)$

we have $\Gamma_1(N)\tau = \Gamma_1(N)\tau'$.

We have shown

① If $\Gamma_1(N)\tau = \Gamma_1(N)\tau'$, then $[\mathbb{C}/\Lambda_\tau, 1/N + \Lambda_\tau] = [\mathbb{C}/\Lambda_{\tau'}, 1/N + \Lambda_{\tau'}]$

② If $[\mathbb{C}/\Lambda_\tau, 1/N + \Lambda_\tau] = [\mathbb{C}/\Lambda_{\tau'}, 1/N + \Lambda_{\tau'}]$, then $\Gamma_1(N)\tau = \Gamma_1(N)\tau'$

$\therefore\ \psi_1 : [\mathbb{C}/\Lambda_\tau, 1/N + \Lambda_\tau] \longmapsto \Gamma_1(N)\tau$ is bijective.

$S_1(N) \cong Y_1(N)$ isomorphic.

$\square$

Recall

Every complex elliptic curve E is isomorphic to the quotient of the complex plane by some lattice Λ_τ ; that is

$$E \cong \mathbb{C}/\Lambda_\tau .$$

→ For proof, look D·S (Diamond, Shurman 1.3)

Lemma 1.3.1

Consider two lattices $\Lambda = \omega_1\mathbb{Z} \oplus \omega_2\mathbb{Z}$ & $\Lambda' = \omega_1'\mathbb{Z} \oplus \omega_2'\mathbb{Z}$ with $\omega_1/\omega_2 \in \mathbb{H}$ & $\omega_1'/\omega_2' \in \mathbb{H}$. Then $\Lambda' = \Lambda$ iff

$$\begin{bmatrix}\omega_1'\\ \omega_2'\end{bmatrix} = \begin{bmatrix}a & b\\ c & d\end{bmatrix}\begin{bmatrix}\omega_1\\ \omega_2\end{bmatrix} \text{ for some } \begin{bmatrix}a & b\\ c & d\end{bmatrix} \in SL_2(\mathbb{Z})$$