"Modular curves over $\mathbb{Q}$ (and $\mathbb{Z}$)" 3/12/12

Fix $N \in \mathbb{Z}_{>0}$, $\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) : c \equiv 0 \bmod N \right\}$

Define

$$\begin{array}{ccc} Y_0(N) = \Gamma_0(N) \backslash \mathbb{H} & \xrightarrow{\text{compactify}} & X_0(N) = \Gamma_0(N) \backslash (\mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})) \\ \downarrow & & \downarrow \text{ramified cover} \\ Y(1) = SL_2(\mathbb{Z}) \backslash \mathbb{H} & \longrightarrow & X(1) = SL_2(\mathbb{Z}) \backslash (\mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})) \end{array}$$

$X_0(N)$ and $X(1)$ are compact Riemann surfaces and are therefore algebraic curves$/\mathbb{C}$.

Attached to each $\tau \in \mathbb{C} \longrightarrow$ is the lattice $\mathbb{Z} + \mathbb{Z}\tau = \Lambda_\tau$
which defines an elliptic curve $E_\tau = \mathbb{C}/\Lambda_\tau$
with a Weierstrass equation $y^2 = 4x^3 - g_2(\tau)x - g_3(\tau)$
There is a j-function $j : \underset{\underset{Y(1)}{\parallel}}{SL_2(\mathbb{Z}) \backslash \mathbb{H}} \longrightarrow \mathbb{C}$ $\quad j(\tau) = \dfrac{1728\, g_2(\tau)^3}{g_2(\tau)^3 - 27 g_3(\tau)^2}$

This is in fact an algebraic ~~ℝ~~ map and identifies

$$\begin{array}{ccc} X(1) & \xrightarrow{\;j\;} & \mathbb{P}^1_{\mathbb{C}} \\ \cup & & \cup \\ Y(1) & \xrightarrow{\sim} & \mathbb{A}^1_{\mathbb{C}} = \operatorname{Spec} \mathbb{C}[j] \end{array}$$

Over any field k, there is an equivalence (of categories)

$$\left\{ \begin{array}{l} \text{smooth projective} \\ \text{curves } /k \\ \text{(geometrically connected} \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{l} \text{Fields } K/k \text{ of transcendence} \\ \text{degree 1 (i.e.} \\ K \cap \bar{k} = k \end{array} \right\}$$

$$C \longmapsto K(C)$$

$\mathbb{C}(X(1)) = \mathbb{C}(j) \subset \mathbb{C}(X_0(N))$ is a finite extension.

Let $S_N = \left\{ \underset{\underset{M_2(\mathbb{Z}_{\geq 0})}{\cap}}{\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}} : ad = N,\ 0 \leq b < d,\ \gcd(a,b,d) = 1 \right\}$

This is a set of coset representatives for $SL_2(\mathbb{Z}) \begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix} SL_2(\mathbb{Z}) = \bigsqcup_{\alpha \in S_N} SL_2(\mathbb{Z})\alpha$.

Let $\Phi_N(x) = \prod_{\alpha \in S_N} (x - j(\alpha(\tau))) = \sum_m s_m(\tau) x^m$

<u>Thm:</u> (a) $s_m(\tau)$ are modular functions of level 1 (i.e. invariant under $SL_2(\mathbb{Z})$)

$\Rightarrow s_m(\tau) \in \mathbb{C}[j]$

and their Fourier coefficients lie in $\mathbb{Z}$

(b) $\Phi_N(x) \in \mathbb{Z}[j][x]$

(c) $j_N(\tau) := j(N\tau) := j\left(\begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix} \tau\right)$ is a modular function of level $\Gamma_0(N)$ and $\Phi_N(j_N) = 0$.

(d) $\Phi_N(x)$ is irreducible over $\mathbb{C}(j)$ and we have $\mathbb{C}(X_0(N)) = \mathbb{C}(j, j_N)$

This allows us to define <u>models</u> for $X_0(N)$ & $X(1)$ over $\mathbb{Q}$.

Why do we want this model?

The <u>j-invariant</u> can be attached to an elliptic curve over any <u>field</u>.

$E: y^2 = 4x^3 - ax - b$ then $j(E) = \dfrac{1728 a^3}{a^3 - 27b^2}$

<u>Fact:</u> $E_1 \simeq E_2$ (over $k = \bar{k}$) $\Longleftrightarrow j(E_1) = j(E_2)$

Take $X(1) = \mathbb{P}^1_{\mathbb{Q}} \supset \mathbb{A}^1_{\mathbb{Q}} = Y(1)$

$\mathbb{A}^1_{\mathbb{Q}} = \operatorname{Spec} \mathbb{Q}[j]$

Then $X_0(N)$ has a model over $\mathbb{Q}$, we let $\mathbb{Q}(X_0(N)) = \mathbb{Q}(j, j_N)$ taken now as a root of the polynomial.

$= \dfrac{\mathbb{Q}(j)[X]}{(\Phi_N(X))}$

$$\begin{tikzcd} & X_0(N) \arrow[dl, "\pi_1"', "j"] \arrow[dr, "\pi_2", "j_N"'] & \\ X(1) & & X(1) \end{tikzcd}$$

This diagram (which we've seen before) now holds over $\mathbb{Q}$.

$Y_0(N)$ = preimage of $Y(1)$ in $X_0(N)$.

parametrizes (E, C) where
- E is an elliptic curve
- $C \subset E[N]$ is a cyclic subgroup of rank N.

So the above diagram (affine part) can be described in terms of the above parametrization:

$$\begin{tikzcd}[column sep=small] (E,C) \arrow[d, mapsto] & & X_0(N) \arrow[dl, "\pi_1"'] \arrow[dr, "\pi_2"] & & (E,C) \arrow[d, mapsto] \\ E & X(1) & & X(1) & E/C \end{tikzcd}$$

(diagram makes sense over $\mathbb{Q}$)

Pick a prime p coprime to N. We have a similar diagram:

$$\begin{tikzcd}[column sep=small] (E, C_N, C_p) \arrow[d, mapsto] & & X_0(Np) \arrow[dl, "\pi_1"'] \arrow[dr, "\pi_2"] & & (E, C_N, C_p) \arrow[d, mapsto] \\ (E, C_N) & X_0(N) & & X_0(N) & (E/C_p, \underbrace{C_N (\mathrm{mod}\ C_p)}_{\text{image}}) \end{tikzcd}$$

(again, diagram makes sense over $\mathbb{Q}$)

Let $J_0(N)$ denote the jacobian of $X_0(N)$

It is an abelian variety parametrizing degree 0 divisor classes on $X_0(N)$

These sorts of diagrams are called <u>correspondences</u>. They give maps of jacobians:

$$T_p := \pi_{2*}\pi_1^* : J_0(N) \longrightarrow J_0(N) \text{ induced by}$$

$$(E, C) \longmapsto \sum_{C_p \in E[p]} (E/C_p, C_N (\mathrm{mod}\ C_p))$$

$$\underbrace{H^0(X_0(N), \Omega^1_{X(N)})}_{\text{wt 2 level } \Gamma_0(N) \text{ modular forms}}{}^{\vee} = (J_0(N))$$

<u>Integral models</u>

$Y(1) \subset X(1)$ has a natural model

Write $Y(1)_{\mathbb{Z}} \subset X(1)_{\mathbb{Z}}$

$$\begin{array}{ccc} Y(1)_{\mathbb{Z}} & \subset & X(1)_{\mathbb{Z}} \\ \| & & \| \\ \mathbb{A}^1_{\mathbb{Z}} & \subset & \mathbb{P}^1_{\mathbb{Z}} \end{array}$$

$Y_0(N)$ has a good model over $\mathbb{Z}[\frac{1}{N}]$ (use the same description eventually)

Why invert N?

Because p-torsion does not behave well mod p.

If E is an elliptic curve over $\overline{\mathbb{F}_p}$, then

$$E(\overline{\mathbb{F}_p})[p] = \begin{cases} \mathbb{Z}/p\mathbb{Z} & \underline{\text{ordinary}} \\ 0 & \underline{\text{supersingular}} \end{cases}$$

We want a correspondence $X_0(Np) \rightrightarrows X_0(N)$ over $\mathbb{Z}[\frac{1}{N}]$.

Over $\mathbb{F}_p$, we have the Frobenius substitution $x \longmapsto x^p$

If $E: y^2 = 4x^3 - ax - b$ is an ell curve, define the <u>Frobenius twist of E</u>

$E^{(p)}: y^2 = 4x^3 - a^p x - b^p$

We have a map $E \xrightarrow{F} E^{(p)}$, $(x,y) \longmapsto (x^p, y^p)$
which is a <u>purely inseparable homomorphism of degree p</u>.

If we take the kernel (as schemes$/_{\overline{\mathbb{F}_p}}$) $F^{-1}(0) = \ker F = \operatorname{Spec} R$, where $R^{red} = \overline{\mathbb{F}_p}$

$\Rightarrow (\ker F)(\overline{\mathbb{F}_p}) = \{O\}$

V = Ver...g

We also have a map $V: E^{(p)} \longrightarrow E$ s.t.:
$FV = VF = p$, and E is supersingular $\Leftrightarrow$ V is purely inseparable
$\Leftrightarrow E \cong E^{(p^2)} = (E^{(p)})^{(p)}$

(With this in mind,) Instead of considering cyclic subgroups $C_p \subset E[p]$, we will consider isogenies $E \longrightarrow E'$ of degree p.

$Y_0(Np)_{\mathbb{Z}[\frac{1}{N}]}$ parametrizes (E, C_N, α) where
- E is an elliptic curve
- C_N is a cyclic subgroup of $E[N]$
- $\alpha: E \longrightarrow E'$ is a p-isogeny.

So then we have the diagram

$$\begin{tikzcd}
& X_0(Np)_{\mathbb{Z}[\frac{1}{N}]} \ni (E, C_N, \alpha) \arrow[dl] \arrow[dr] & \\
X_0(N) \ni (E, C_N) & & (E', \alpha(C_N)) \in X_0(N)
\end{tikzcd}$$

where $X_0(Np)_{\mathbb{Z}[1/N]}$ (or $X_0(N)$) is the normalization of $X(1)_{\mathbb{Z}[1/N]}$ in $Y_0(Np)_{\mathbb{Z}[1/N]}$ (or $Y_0(N)$)

<u>Fact</u>: $X_0(N)_{\mathbb{F}_p}$ is a smooth projective curve, but $X_0(Np)_{\mathbb{F}_p}$ is not quite smooth.

Consider the ordinary locus of $X_0(Np)_{\mathbb{F}_p}$, $X_0(Np)^{ord}_{\mathbb{F}_p} = \{(E, C_N, \alpha) \in X_0(Np) : E \text{ is ordinary}\}$
<u>Note</u>: π_1, π_2 takes ordinary locus to ordinary locus.

E, ordinary elliptic curve over $\overline{\mathbb{F}_p}$ has 2 p-isogenies
- $E \xrightarrow{F} E^{(p)}$
- $E \xrightarrow{V^{(p^{-1})}} E^{(p^{-1})}$

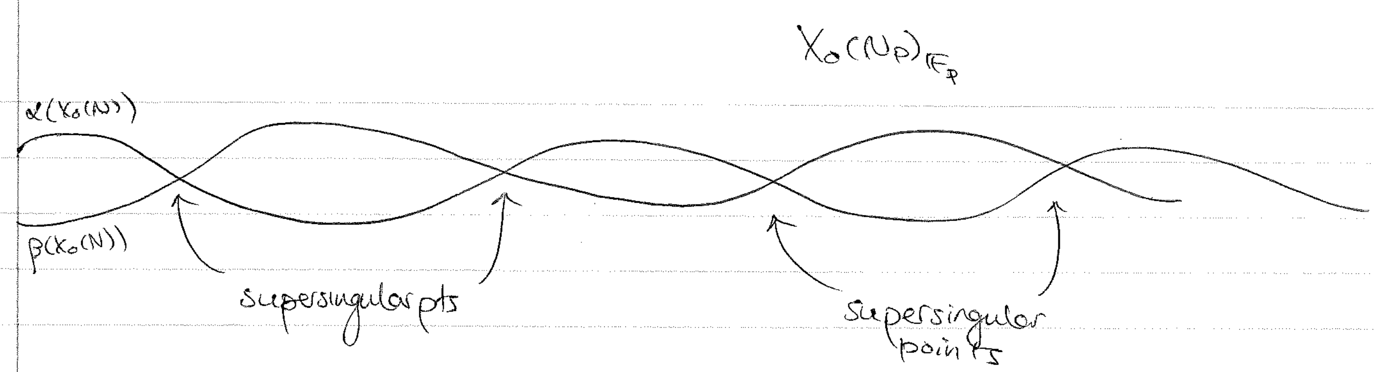
} distinct.

Now consider the following diagram:

$$\begin{tikzcd}
X_0(N)^{ord}_{\mathbb{F}_p} \ni (E,C) \arrow[dr, "\alpha"] \arrow[ddd, bend right] & & X_0(N)^{ord}_{\mathbb{F}_p} \ni (E,C) \arrow[dl, "\beta"'] \arrow[ddd, bend left] \\
& X_0(Np)^{ord} \ni (E,C,F),\ (E^{(p)}, C^{(p)}, V) \arrow[ddl, "\pi_1"] \arrow[ddr, "\pi_2"'] & \\
& & \\
X_0(N)^{ord}_{\mathbb{F}_p} & & X_0(N)^{ord}_{\mathbb{F}_p}
\end{tikzcd}$$

$\pi_1 \circ \alpha = id$. $\qquad \pi_2 \circ \beta = id$.

$X_0(N)^{ord}_{\mathbb{F}_p} = \alpha(X_0(N)^{ord}_{\mathbb{F}_p}) \sqcup \beta(X_0(N)^{ord}_{\mathbb{F}_p})$



Consider $\pi_2 \circ \alpha = \pi_1 \circ \beta : X_0(N)^{ord}_{\mathbb{F}_p} \longrightarrow X_0(N)^{ord}_{\mathbb{F}_p}$

$$(E, C) \longmapsto (E^{(p)}, C^{(p)})$$

Now restrict the previous diagram to image of α, β:

$$\begin{tikzcd} & \alpha(X_0(N)^{ord}) \arrow[dl, "id"'] \arrow[dr, "F"] & \\ X_0(N) & & X_0(N) \end{tikzcd} \qquad \begin{tikzcd} & \beta(X_0(N)^{ord}) \arrow[dl, "F"'] \arrow[dr, "id"] & \\ X_0(N) & & X_0(N) \end{tikzcd}$$

$$T_p = F_* \qquad\qquad T_p = F^*$$

We get the Eichler-Shimura relation (on the ordinary locus, which is dense)

$$T_p = F_* + F^*$$