Geometry of $X(N,p)$ over $\mathbb{Z}_p$

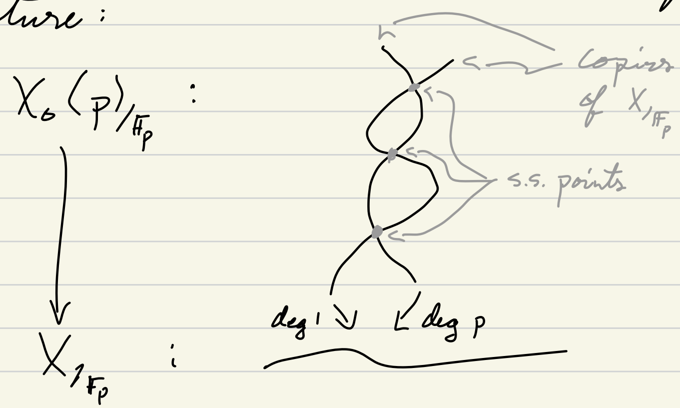
HHT Seminar
Columbia University
Summer 2021

§1 – Main Result

Let p = prime, $N \geq 4$, $p \nmid N$.

Let X = Modular curve for $\Gamma_1(N)$ and
$X_0(p)$ = ——————————— $\Gamma_1(N) \cap \Gamma_0(p)$

We want to understand the following picture:



This picture is about compact modular curve but we will mostly talk about the affine ones & ignore cusps for a little bit.

Plan:
- Moduli Problems
- Elliptic Curves in char p
- Main result

§2 - Moduli Problems

Let ELL be the category

Obj: $E \to S$, where

1. S = scheme
2. E = S-group scheme
3. all geometric fibres are elliptic curves

Morphism:
$$\begin{tikzcd} E' \arrow[r] \arrow[d] & E \arrow[d] \\ S \arrow[r] & S' \end{tikzcd}$$
s.t. $E' \cong E \times_S S'$

Definition A moduli problem $\mathcal{P}$ is a set pre-sheaf on ELL

E.g. $[\Gamma_1(N)](E/S) = \{\Gamma_1(N)\text{-level structure on } E/S\}$

$[\Gamma_0(N)](E/S) = \{\Gamma_0(N)\text{-level structure on } E/S\}$

In general, $\alpha \in \mathcal{P}(E/S)$ is called $\mathcal{P}$-level structure on E/S.

We will care later about

$$\mathcal{P} = [\Gamma_1(N)] \times [\Gamma_0(p)]$$

§2.1 – Moduli Spaces & Univ. Elliptic Curves

If $\mathcal{P}$ is representable, the representing object is an elliptic curve

$$\begin{tikzcd} \mathbb{E} \arrow[d, "\pi"] \\ \mathcal{M}(\mathcal{P}) \arrow[u, bend left, "e"] \end{tikzcd}$$

and we say $\mathbb{E}$ = Universal elliptic curve

$\mathcal{M}(\mathcal{P})$ = Moduli space for $\mathcal{P}$

Remark The scheme $\mathcal{M}(\mathcal{P})$ represents the functor

$$\mathrm{SCH} \longrightarrow \mathrm{SETS}$$

$$S \mapsto (E/S, \alpha), \text{ where}$$

1. $E/S \in \mathrm{ELL}$
2. $\alpha \in \mathcal{P}(E/S)$

by considering pull-backs across $S \to \mathcal{M}(\mathcal{P})$

This gives rise to the important line bundle

$$\omega := \pi_* \Omega^1_{\mathbb{E}/\mathcal{M}(\mathcal{P})}$$

$$= e^* \Omega^1_{\mathbb{E}/\mathcal{M}(\mathcal{P})}$$

§2.2 - Analysis of $\mathcal{P} = [\Gamma_1(N)]$

Proposition The moduli problem $[\Gamma_1(N)]$ is *relatively representable*, i.e.

"For all E/S, the functor

$$[\Gamma_1(N)]_{E/S} : SCH_{/S} \to SETS$$
$$T \mapsto [\Gamma_1(N)](E \times_S T/T)$$

is representable"

Proof We can take the *finite, étale* S-scheme

$$T = S \times \left\{ \begin{array}{l} \text{elements of } (\mathbb{Z}/N\mathbb{Z})^2 \text{ of} \\ \text{exact order } N \end{array} \right\}$$

closed subscheme of $(\mathbb{Z}/N\mathbb{Z})^2$

$\square$

Theorem $[\Gamma_1(N)]$ and $[\Gamma_1(N)] \times [\Gamma_0(p^n)]$ are both representable.

Also, $X = \mathcal{M}([\Gamma_1(N)])$ is *smooth* and $X_0(p^n) = \mathcal{M}([\Gamma_1(N)] \times [\Gamma_0(p^n)])$ is a *finite flat* cover of X

Proof For $N \geq 4$, $[\Gamma_1(N)]$ is *rigid*. The above + this fact $\Rightarrow$ representable.

For second part, $[\mathcal{P}_0(p^n)]$ is also relatively representable. Then, take

$$X_0(p^n) = \text{Scheme representing } [\mathcal{P}_0(p^n)]_{E/X} \qquad \square$$

§3 - Elliptic Curves in Characteristic p

§3.1 - Frobenius & Verschiebung

Let $S = \mathbb{F}_p$-scheme, then we have an absolute Frobenius

$$\begin{tikzcd} F_{abs} : S \arrow[rr] \arrow[dr] & & S \arrow[dl] \\ & \operatorname{Spec} \mathbb{F}_p & \end{tikzcd} \qquad (\varphi \mapsto \varphi^p)$$

Now, if $X = S$-scheme (we write $X/S/\mathbb{F}_p$), then

$$\begin{tikzcd} X \arrow[r, dashed, "F_{X/S}"] \arrow[rr, bend left, "F_{abs}"] \arrow[dr, bend right] & X^{(p)} \arrow[r] \arrow[d] \arrow[dr, phantom, "\lrcorner", very near start] & X \arrow[d] \\ & S \arrow[r, "F_{abs}"] & S \end{tikzcd}$$

and $F_{X/S}$ = (relative) Frobenius

When X/S is an elliptic curve E/S, we get an isogeny of degree p

$$F_{E/S} : E \to E^{(p)},$$

Definition The dual isogeny is
$$V_{E/S} : E^{(p)} \longrightarrow E,$$
called *Verschiebung*.

We can iterate them to get
$$F^n : E \to E^{(p^n)} \quad ; \quad V^n : E^{(p^n)} \longrightarrow E$$
and obviously, $p^n = V^{(n)} \circ F^{(n)}$, so
$$0 \to \ker(F^n) \longrightarrow E[p^n] \longrightarrow \ker(V^n) \to 0$$

Fact / Definition

1. Let $P \in E[p^n](S)$

P *generates* $E[p^n] \iff F^n(P)$ *generates* $\ker(V^n)$

2. A generator of $\ker(V^n)$ is called an *Igusa structure of level p^n* on E/S.

It leads to moduli problem
$$[\mathrm{Ig}(p^n)](E/S) = \{\text{Gen's of } \ker(V^n)\}$$

Remark If E is ordinary (see below),

$$\begin{array}{c}\text{Generators}\\ \text{of } \ker(V^n)\end{array} \xleftrightarrow{1:1} \begin{array}{c}\text{Isomorphisms}\\ \mathbb{Z}/p^n\mathbb{Z} \xrightarrow{\sim} E[p^n]^{et}\end{array}$$

Over $S = \mathrm{Spec}(k)$ w/ $k = \bar{k}$, the situation is as usual

Proposition Let $P \in E^{(p)}(k)$ be a generator (as a Cartier divisor) of $\ker(V)$

Then, either:

1) $P = 0$ and so, 0 generates all $\ker(V^n)$

2) $P \neq 0$ and V^n is étale & $\ker(V^n) \cong \mathbb{Z}/p^n\mathbb{Z}$

In case 1), E/k is supersingular.
In case 2), E/k is ordinary.

Definition In general, $E/S/\mathbb{F}_p$ is ordinary if all geometric fibers are ord.

Otherwise, it is supersingular

Definition The "ordinary" moduli problem is

$$[\mathrm{ord}] : \mathrm{ELL}_{/\mathbb{F}_p} \longrightarrow \mathrm{SETS}$$

$$E/S/\mathbb{F}_p \longmapsto \begin{cases} \{*\}, & \text{if } E \text{ is ordinary} \\ \emptyset, & \text{if } E \text{ is s.s.} \end{cases}$$

Prop $[\mathrm{ord}]$ is relatively representable, affine and open.

Proof Consider non-vanishing locus of Hasse inv. $\square$

Remark As we saw before, if $\mathcal{P}$ is a *representable* moduli problem, so is $\mathcal{P}^{\mathrm{ord}} := \mathcal{P} \times [\mathrm{ord}]$.

The scheme $\mathcal{M}(\mathcal{P})^{\mathrm{ord}} := \mathcal{M}(\mathcal{P}^{\mathrm{ord}})$ is an open subscheme of $\mathcal{M}(\mathcal{P})$, called its *ordinary locus*.

§3.2 – Classifying p^n-isogenies

Proposition Let $E_0/S/\mathbb{F}_p$, $E_n/S/\mathbb{F}_p$ be *ordinary* ell. curves, and $\pi : E_0 \to E_n$, a p^n-isogeny.

Let F_0 (resp. V_n) be the *Frobenius* (resp. *Verschiebung*) map on E_0 (resp. E_n). Then,

$$\pi : E_0 \xrightarrow{F_0^a} E_0^{(p^a)} \xrightarrow{\sim} E_n^{(p^b)} \xrightarrow{V_n^b} E_n,$$

for some $a, b \geq 0$ s.t. $a+b=n$.

Proof $\ker(\pi) \cap \ker(F_0^n) = \ker(F_0^a)$, so

$$\pi : E_0 \xrightarrow{F_0^a} E_0^{(p^a)} \xrightarrow{\pi_{a,n}} E_n$$

and $0 \to \ker(F_0^a) \to \ker \pi \to \left(\begin{matrix}\text{étale, cyclic,} \\ \text{order } p^{n-a} = p^b\end{matrix}\right) \to 0$

$\Rightarrow$ Dual $\pi_{a,n}^\vee : E_n \to E_0^{(p^a)}$ is a p^b-isogeny w/ kernel $\mu_{p^b} = \ker(F^b)$.

$\Rightarrow \pi_{a,n}^\vee : E_n \longrightarrow E_n^{(p^b)} \xrightarrow{\sim} E_0^{(p^a)}$ ◻

Definition If π is as above, we say it is of *type* (a,b)

We say it is *(a,b)-cyclic* if $a=0$, $b=0$ OR

$\exists$ closed $T \subset S$ defined by ideal $\mathcal{I}$ s.t. $\mathcal{I}^{p-1} = 0$, and the isom. $E_0^{(p^a)} \cong E_n^{(p^b)}$, restricted to T, is induced by some isom. $E_0^{(p^{a-1})} \cong E_n^{(p^{b-1})}$.

Definition A finite flat subgp $G \subset E$ of rank p^n is of *type (a,b)* or *(a,b)-cyclic* if the proj. $\pi : E \to (E/G)$ is.

These naturally induce moduli problems $[(a,b)]$ and $[(a,b)\text{-cyc}]$, as well as

$$[\mathcal{P}, (a,b)] := \mathcal{P} \times [(a,b)]$$

$$[\mathcal{P}, (a,b)\text{-cyc}] := \mathcal{P} \times [(a,b)\text{-cyc}]$$

Theorem Let k be perfect, $\operatorname{char} k = p$, $\mathcal{P}$ *representable* on (Ell/k), finite étale. Fix $a+b=n$.

Then, $[\mathcal{P}, (a,b)\text{-cyc}]$ is *representable* by a finite flat $\mathcal{M}(\mathcal{P})$-scheme of *degree*

$$\begin{cases} \phi(p^b), & \text{if } a \neq 0 \\ p^b, & \text{if } a = 0 \end{cases}$$

Also, $\mathcal{M}(\mathcal{P}, (a,b)\text{-cyc})(A) \to \mathcal{M}(\mathcal{P})(A)$ is bijective for any *perfect* k-algebra A.

Finally, the "forget (a,b)" map

$$\mathcal{M}(\mathcal{P}, (a,b)\text{-cyc}) \to \mathcal{M}(\mathcal{P}, [\Gamma_0(p^n)])$$

is a closed immersion.

Proof Let $\sigma : k \to k$ be abs. Frobenius.
For any $i \in \mathbb{Z}_{\geq 0}$, let $S^{(\sigma^i)} := S \otimes_{k, \sigma^i} k$ for any k-scheme S.

For $a = 0$ or $b = 0$, the following

$$\mathcal{M}(\mathcal{P}, (a,b)\text{-cyc}) := (F^a \times F^b)^{-1}(\Delta),$$

where

$$F^a \times F^b : \mathcal{M}(\mathcal{P}) \times_k \mathcal{M}(\mathcal{P})^{(\sigma^{a-b})} \to \mathcal{M}(\mathcal{P})^{(\sigma^a)} \times_k \mathcal{M}(\mathcal{P})^{(\sigma^a)}$$

works. For $a, b \neq 0$, needs modification. $\square$

§4 - Crossing Theorem

§4.1 - Picture

Consider $\mathcal{P} = [\Gamma_1(N)]$ (repr'ble, finite, étale)

$$\begin{tikzcd}
\underset{X_0(p^n)}{\mathcal{M}(\mathcal{P}, [\Gamma_0(p^n)])} \arrow[d, "\text{finite flat}"] & \coprod_{a+b=n} \underset{X_{a,b}}{\mathcal{M}(\mathcal{P}, (a,b)\text{-cyc})} \arrow[l, "\text{each}"', "\text{cl. imm.}"] \arrow[ddl, "\text{each finite flat}"] \\
\mathcal{M}(\mathcal{P}) = X \arrow[d, "\text{smooth}"] & \\
\operatorname{Spec}(k) &
\end{tikzcd}$$

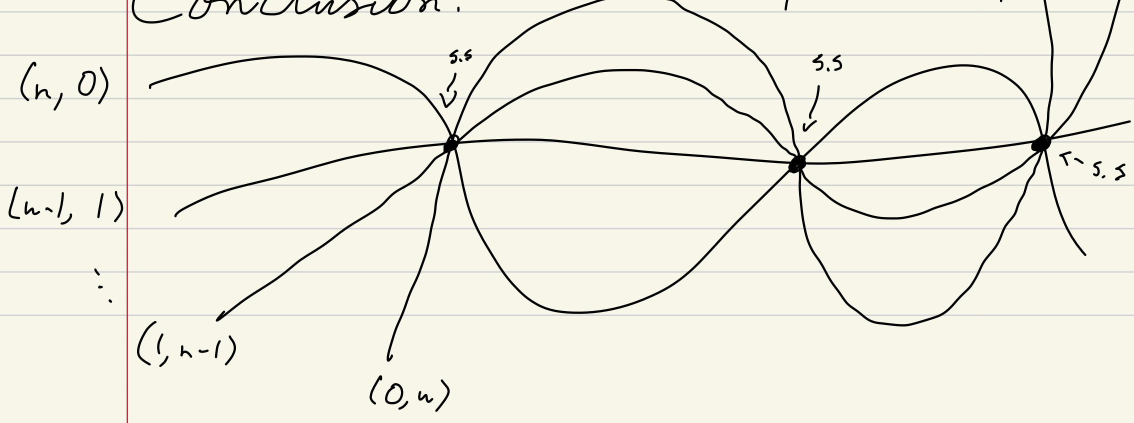
($k = \mathbb{F}_p$-ext^n, perfect)

1) Supersingular $\overset{\text{geometric}}{}$ points of X lift uniquely to $X_0(p^n)$ and to each $X_{a,b}$

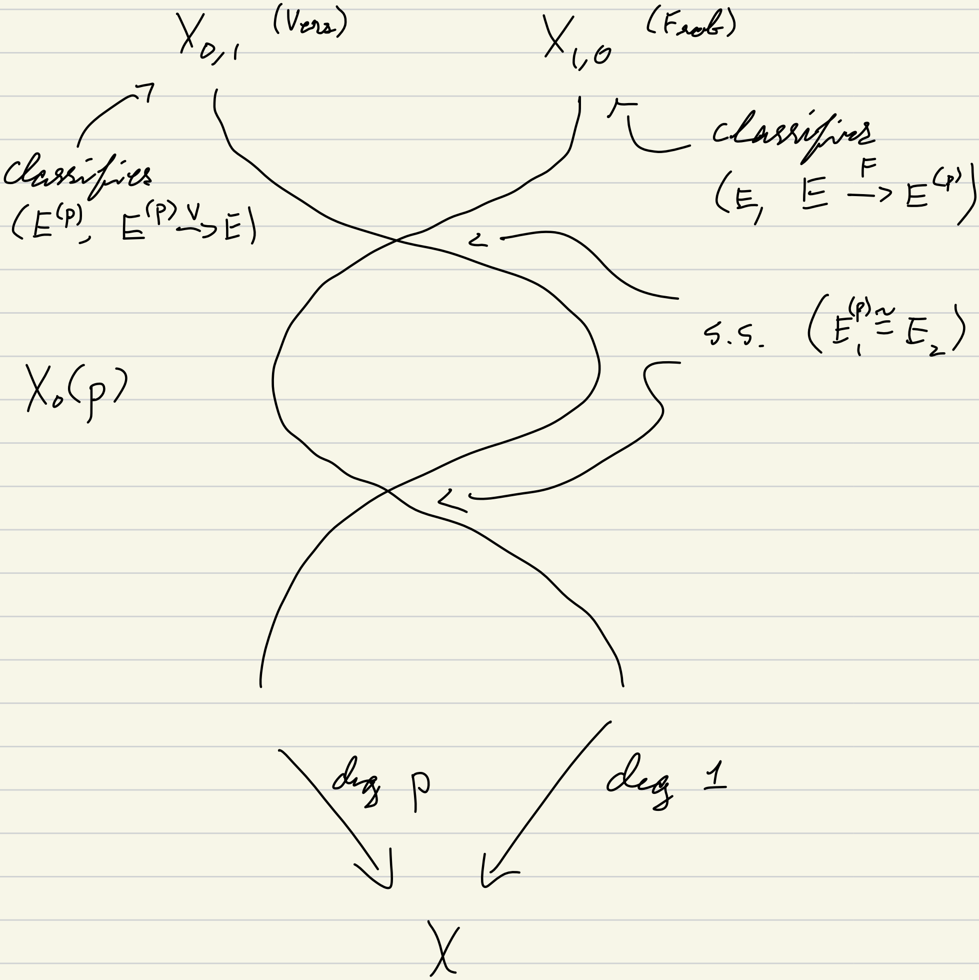
2) Away from s.s. points, $\coprod X_{a,b} \to X_0(p^n)$ is an isom.

Conclusion:

$X_0(p^n)$ looks like:



For $n=1$, only $(1,0)$ & $(0,1)$, so



This picture extends w/o problems to cusps by compactifying.

Even the universal ell. curve $\underline{E} \to \mathcal{M}(p)$ extends to a semi-abelian curve.