Serre’s Uniformity Conjecture

Conjecture (Serre’s Uniformity Conjecture)

Let $E/\mathbb{Q}$ be without CM. Let $p > 37$. Then $\bar{\rho}_{E,p}$ is surjective.

Note: $\bar{\rho}$ surjective $\iff$ image contains $\text{SL}_2(\mathbb{F}_p)$.

Theorem (Dickson)

Let $H$ be a subgroup of $\text{GL}_2(\mathbb{F}_p)$ not containing $\text{SL}_2(\mathbb{F}_p)$. Then (up to conjugation)

(i) either $H \subseteq B_0(p) := \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\}$ (Borel subgroup)

(ii) or $H \subseteq N_s^+(p) := \left\{ \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix}, \begin{pmatrix} 0 & \alpha \\ \beta & 0 \end{pmatrix} : \alpha, \beta \in \mathbb{F}_p^* \right\}$ (normalizer of split Cartan)

(iii) or $H \subseteq N_{ns}^+(p)$ (normalizer of non-split Cartan).

(iv) or the image of $H$ in $\text{PGL}_2(\mathbb{F}_p)$ is isomorphic to $A_4$, $S_4$ or $A_5$ (these are called the exceptional subgroups of $\text{GL}_2(\mathbb{F}_p)$).
Vague Objective

Given
- a field $K$,
- a positive integer $N$,
- and a subgroup $H \subseteq \text{GL}_2(\mathbb{Z}/N\mathbb{Z})$,

want to understand

\[ (*) \{ \text{elliptic curves } E/K : \bar{\rho}_{E,N}(G_K) \text{ is conjugate to a subgroup of } H \} \, . \]

There is a modular curve $X_H$ associated to $H$.

Provided $H$ satisfies certain technical assumptions,
- elements of (*) give rise to (non-cuspidal) $K$-points on $X_H$.
- By understanding $X_H(K)$ we can give a complete description of the set (*).
Modular Curves corresponding to subgroups of $\text{GL}_2(\mathbb{F}_p)$

Corresponding to six groups $B_0(p), N_s^+(p), N_{ns}^+(p), A_4, S_4, A_5$ in Dickson’s classification are six modular curves $X_0(p), X_s^+(p), X_{ns}^+(p), X_{A_4}(p), X_{S_4}(p)$ and $X_{A_5}(p)$.

To prove Serre’s uniformity conjecture, enough to show that the rational points on each of these curves are either CM or cuspidal for $p > 37$.

**In fact this has been accomplished for all these families except $X_{ns}^+(p)$**.

---

**Theorem (Serre)**

If $p \geq 13$ then $X(\mathbb{Q}_p) = \emptyset$ for $X = X_{A_4}(p), X_{S_4}(p), X_{A_5}(p)$.

---

**Theorem (Mazur)**

If $p > 37$ then $X_0(p)(\mathbb{Q}) \subset \{\text{cusps, cm points}\}$.

---

**Theorem (Bilu, Parent and Rebolledo)**

If $p > 13$ then $X_s^+(p)(\mathbb{Q}) \subset \{\text{cusps, cm points}\}$.
To prove Serre’s uniformity conjecture, enough to show that the rational points on each of these curves are either CM or cuspidal for $p > 37$.

**In fact this has been accomplished for all these families except $X_{ns}^+(p)$.**

**Theorem (Serre)**

*If $p \geq 13$ then $X(\mathbb{Q}_p) = \emptyset$ for $X = X_{A_4}(p), X_{S_4}(p), X_{A_5}(p)$.***

**Theorem (Mazur)**

*If $p > 37$ then $X_0(p)(\mathbb{Q}) \subset \{ \text{cusps, cm points} \}$.***

**Theorem (Bilu, Parent and Rebolledo)**

*If $p > 13$ then $X_s^+(p)(\mathbb{Q}) \subset \{ \text{cusps, cm points} \}$.***

**Theorem (Balakrishnan, Dogra, Müller, Tuitman, Vonk)**

*X_s^+(13)(\mathbb{Q}) and X_{ns}^+(13)(\mathbb{Q}) consist of cusps and CM points.*

The question of rational points on $X_{ns}^+(p)$ is a famous open problem.
The Modular Curve $X(1)$—Recap

\[ \mathbb{H} := \{ x + yi : x, y \in \mathbb{R}, y > 0 \} \quad \text{(upper half-plane)} \]
\[ \mathbb{H}^* := \mathbb{H} \cup \mathbb{P}^1(\mathbb{Q}) \quad \text{(extended upper half-plane)}. \]

- Given any $\tau \in \mathbb{H}$, there is an elliptic curve $E_\tau/\mathbb{C}$ such that $E_\tau(\mathbb{C}) \cong \mathbb{C}/(\mathbb{Z} + \mathbb{Z} \cdot \tau)$.
- Every elliptic curve over $\mathbb{C}$ is isomorphic to $E_\tau$ for some $\tau$.
- Moreover $E_{\tau_1} \cong E_{\tau_2}$ if and only if $\tau_1 = \gamma(\tau_2)$ for some $\gamma \in \text{SL}_2(\mathbb{Z})$.

\[ \therefore \text{we have a bijection} \]
\[ \text{SL}_2(\mathbb{Z}) \backslash \mathbb{H} \leftrightarrow \{ \text{isom classes of elliptic curves } E/\mathbb{C} \}, \]
\[ \text{SL}_2(\mathbb{Z}) \cdot \tau \leftrightarrow [\mathbb{C}/(\mathbb{Z} + \mathbb{Z}\tau)] \quad ([ \cdot ] = \text{isom class}). \]

$\text{SL}_2(\mathbb{Z}) \backslash \mathbb{H}$ is a Riemann surface. Its points are in 1–1 correspondence with isom classes of elliptic curves over $\mathbb{C}$. 
we have a bijection

\[
\begin{align*}
\text{SL}_2(\mathbb{Z}) \setminus \mathbb{H} & \leftrightarrow \{\text{isom classes of elliptic curves } E/\mathbb{C}\}, \\
\text{SL}_2(\mathbb{Z}) \cdot \tau & \mapsto [\mathbb{C}/(\mathbb{Z} + \mathbb{Z}\tau)] \quad ([\cdot] = \text{isom class}).
\end{align*}
\]

- \(\text{SL}_2(\mathbb{Z}) \setminus \mathbb{H}\) is a Riemann surface. Its points are in 1−1 correspondence with isom classes of elliptic curves over \(\mathbb{C}\).
- \(\text{SL}_2(\mathbb{Z}) \setminus \mathbb{H}\) is non-compact; its compactification is \(\text{SL}_2(\mathbb{Z}) \setminus \mathbb{H}^*\) \((\mathbb{H}^* := \mathbb{H} \cup \mathbb{P}^1(\mathbb{Q}))\).
- \(\text{SL}_2(\mathbb{Z}) \setminus \mathbb{H}^*\) is a compact Riemann surface of genus 0.
- The points of \(\mathbb{P}^1(\mathbb{Q}) \subset \mathbb{H}^*\) form one orbit under the action of \(\text{SL}_2(\mathbb{Z})\), so the compactification has only one extra point, called the ‘the \(\infty\) cusp’.
- Any compact Riemann surface can be identified as the set of complex points on an algebraic curve of the same genus.
• $\text{SL}_2(\mathbb{Z}) \backslash \mathbb{H}^*$ is a compact Riemann surface of genus 0.

• The points of $\mathbb{P}^1(\mathbb{Q}) \subset \mathbb{H}^*$ form one orbit under the action of $\text{SL}_2(\mathbb{Z})$, so the compactification has only one extra point, called the ‘the $\infty$ cusp’.

• Any compact Riemann surface can be identified as the set of complex points on an algebraic curve of the same genus.

• In this we case we denote the algebraic curve by $X(1) = \mathbb{P}^1$.

$$j : \text{SL}_2(\mathbb{Z}) \backslash \mathbb{H}^* \to X(1)(\mathbb{C}) ,$$

$$\text{SL}_2(\mathbb{Z}) \cdot \tau \mapsto j(\tau) = \frac{1}{q} + 744 + 196884q^2 + \cdots ,$$

where

$$q := \begin{cases} \exp(2\pi i \tau) & \tau \in \mathbb{H} \\ 0 & \tau \in \mathbb{P}^1(\mathbb{Q}) . \end{cases}$$
In this case we denote the algebraic curve by $X(1) = \mathbb{P}^1$.

$$j : \text{SL}_2(\mathbb{Z}) \backslash \mathbb{H}^* \rightarrow X(1)(\mathbb{C}) ,$$

$$\text{SL}_2(\mathbb{Z}) \cdot \tau \mapsto j(\tau) = \frac{1}{q} + 744 + 196884q^2 + \cdots ,$$

where

$$q := \begin{cases} \exp(2\pi i \tau) & \tau \in \mathbb{H} \\
0 & \tau \in \mathbb{P}^1(\mathbb{Q}). \end{cases}$$

- $j$ sends cusp $\text{SL}_2(\mathbb{Z}) \backslash \mathbb{P}^1(\mathbb{Q})$ to $\infty \in X(1)(\mathbb{C})$.
- Let $Y(1) := X(1) \backslash \infty \cong \mathbb{A}^1$.

**Summary:** There is a 1 − 1 correspondence between isomorphism classes of elliptic curves $E/\mathbb{C}$ and points $j \in Y(1)(\mathbb{C})$ (the value is $j \in Y(1)(\mathbb{C})$ corresponding to $E/\mathbb{C}$ is familiar $j$-invariant $j(E)$).

Now let $K$ be any field. The correspondence between isomorphism classes of $E/K$ and points in $Y(1)(\overline{K})$, sending $E$ to its $j$-invariant $E$, remains valid.
Summary: There is a 1 − 1 correspondence between isomorphism classes of elliptic curves $E/\mathbb{C}$ and points $j \in Y(1)(\mathbb{C})$ (the value is $j \in Y(1)(\mathbb{C})$ corresponding to $E/\mathbb{C}$ is familiar $j$-invariant $j(E)$).

Now let $K$ be any field. The correspondence between isomorphism classes of $E/K$ and points in $Y(1)(\overline{K})$, sending $E$ to its $j$-invariant $E$, remains valid.

Points $j \in Y(1)(K)$ correspond to classes of elliptic curves defined over $K$ which are isomorphic over $\overline{K}$.

If $E, E'$ are defined over $K$ and isomorphic over $\overline{K}$, then they are quadratic twists, except possibly if they have $j$-invariants 0, 1728.

So we have the following 1 − 1 correspondence:

\[
\{\text{elliptic curves over } K \text{ with } j\text{-invariant } \neq 0, 1728\} / \sim \\
\iff j \in X(1)(K) \setminus \{0, 1728, \infty\}
\]

where $\sim$ denotes quadratic twisting.
The modular curves $X_1(N), X_0(N)$

Fix $N \geq 1$.

- Want to understand isomorphism classes of pairs $(E, P)$,
  - where $E$ is an elliptic curve;
  - $P$ is a point of order $N$;
  - $(E, P), (E', P')$ are **isomorphic** if there is an isomorphism $\phi : E \to E'$ with $\phi(P) = P'$.

- Given $(E, P)$ with $E/\mathbb{C}$,
  - $\exists \tau \in \mathbb{H}$ such that $E(\mathbb{C}) \cong \mathbb{C}/(\mathbb{Z} + \mathbb{Z} \cdot \tau)$ AND
  - this isom takes $P$ to $1/N + (\mathbb{Z} + \mathbb{Z} \tau) \in \mathbb{C}/(\mathbb{Z} + \mathbb{Z} \tau)$;
  - We identify $[(E, P)]$ with $[(\mathbb{C}/(\mathbb{Z} + \mathbb{Z} \tau), 1/N)]$;
  - $(\mathbb{C}/(\mathbb{Z} + \mathbb{Z} \tau_1), 1/N) \cong (\mathbb{C}/(\mathbb{Z} + \mathbb{Z} \tau_2), 1/N)$ iff $\exists \gamma \in \Gamma_1(N)$ such that $\tau_1 = \gamma(\tau_2)$.

$\Gamma_1(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}_2(\mathbb{Z}) : a \equiv d \equiv 1 \pmod{N}, \ c \equiv 0 \pmod{N} \right\}$.

Obtain 1 – 1 correspondence

\[
\Gamma_1(N) \backslash \mathbb{H} \leftrightarrow \{ \text{isom classes of pairs } (E/\mathbb{C}, P) \}, \\
\Gamma_1(N) \cdot \tau \leftrightarrow [(\mathbb{C}/(\mathbb{Z} + \mathbb{Z} \tau), 1/N)].
\]
Also want to understand isomorphism classes of pairs \((E, C)\) where
\begin{itemize}
  \item \(E/C\) is an elliptic curve;
  \item \(C\) is a cyclic subgroup of order \(N\);
  \item pairs \((E_1, C_1), (E_2, C_2)\) are isomorphic if there exists isomorphism 
  \(\phi : E_1 \to E_2\) such that \(\phi(C_1) = C_2\).
  \item Write \([((E, C))]\) for the isomorphism class of the pair \((E, C)\).
\end{itemize}

Obtain 1–1 correspondence
\[
\Gamma_0(N) \backslash \mathbb{H} \leftrightarrow \{\text{isom classes of pairs } (E/C, C)\},
\]
\[
\Gamma_0(N) \cdot \tau \mapsto \left[ ((C/(\mathbb{Z} + \mathbb{Z}\tau), \langle 1/N \rangle) \right].
\]

where
\[
\Gamma_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}_2(\mathbb{Z}) : c \equiv 0 \pmod{N} \right\}.
\]

Miracle: there are (open) curves \(Y_1(N), Y_0(N)\) defined over \(\mathbb{Q}\), such that
\[
Y_1(N)(\mathbb{C}) \cong \Gamma_1(N) \backslash \mathbb{H}, \quad Y_0(N)(\mathbb{C}) \cong \Gamma_0(N) \backslash \mathbb{H},
\]

The completions \(X(1), X_1(N), X_0(N)\) satisfy
\[
X_1(N)(\mathbb{C}) \cong \Gamma_1(N) \backslash \mathbb{H}^*, \quad X_0(N)(\mathbb{C}) \cong \Gamma_0(N) \backslash \mathbb{H}^*.
\]
Miracle: there are (open) curves \(Y_1(N), Y_0(N)\) defined over \(\mathbb{Q}\), such that
\[
Y_1(N)(\mathbb{C}) \cong \Gamma_1(N)\backslash \mathbb{H}, \quad Y_0(N)(\mathbb{C}) \cong \Gamma_0(N)\backslash \mathbb{H},
\]
The completions \(X(1), X_1(N), X_0(N)\) satisfy
\[
X_1(N)(\mathbb{C}) \cong \Gamma_1(N)\backslash \mathbb{H}^*, \quad X_0(N)(\mathbb{C}) \cong \Gamma_0(N)\backslash \mathbb{H}^*,
\]
We call \(X_1(N) \setminus Y_1(N), X_0(N) \setminus Y_0(N)\) the sets of \textbf{cusps} of \(X_1(N), X_0(N)\) respectively.

Facts.

- A point \(Q \in Y_1(N)(\overline{K})\) parametrises an isomorphism class of pairs \([(E, P)]\) where \(E/\overline{K}\) and \(P\) is a point of order \(N\). We write \(Q = [(E, P)] \in Y_1(N)(\overline{K})\) (i.e. identify point \(Q \in Y_1\) with pair it represents).
- This parametrisation is compatible with the action of \(G_K\). Thus \(Q^\sigma = [(E, P)]^\sigma\) where \([(E, P)]^\sigma\) is simply defined as \((E^\sigma, P^\sigma)\).
- Let \(Q = [(E, P)] \in Y_1(N)(\overline{K})\) as above. If \(E\) is defined over \(K\), and \(P\) is a \(K\)-rational point of order \(N\), then \(Q^\sigma = [(E, P)]^\sigma = [(E, P)] = Q\) for all \(\sigma \in G_K\), and thus \(Q \in Y_1(K)\).
The Modular Curve $X_H$

We want to generalise previous constructions to an arbitrary group $H \leq \text{GL}_2(\mathbb{Z}/N\mathbb{Z})$.

- An isomorphism $\alpha : E[N] \rightarrow (\mathbb{Z}/N\mathbb{Z})^2$ a level $N$ structure on $E$.
- A level $N$-structure is same as choice of basis for $E[N]$: $P = \alpha^{-1}(e_1)$, $Q = \alpha^{-1}(e_2)$ where $e_1 = (1, 0)$, $e_2 = (0, 1)$.
- We call pairs $(E_1, \alpha_1)$ and $(E_2, \alpha_2)$ $H$-isomorphic, and write

  $$(E_1, \alpha_1) \sim_H (E_2, \alpha_2)$$

  if there is an isom $\phi : E_1 \rightarrow E_2$ and an element $h \in H$ such that

  $$\alpha_1 = h \circ \alpha_2 \circ \phi$$

  (think of $h \in H$ as $h : (\mathbb{Z}/N\mathbb{Z})^2 \cong (\mathbb{Z}/N\mathbb{Z})^2$).

**Exercise.** Show that $H$-isomorphism is an equivalence relation. We denote the $H$-isomorphism class of the pair $(E, \alpha)$ by $[(E, \alpha)]_H$. 
We want to generalise previous constructions to an arbitrary group \( H \leq \text{GL}_2(\mathbb{Z}/N\mathbb{Z}) \).

- An isomorphism \( \alpha : E[N] \to (\mathbb{Z}/N\mathbb{Z})^2 \) is a level \( N \) structure on \( E \).

- A level \( N \)-structure is same as choice of basis for \( E[N] \): \( P = \alpha^{-1}(e_1), Q = \alpha^{-1}(e_2) \) where \( e_1 = (1, 0), e_2 = (0, 1) \).

- We call pairs \((E_1, \alpha_1)\) and \((E_2, \alpha_2)\) \( H \)-isomorphic, and write

\[
(E_1, \alpha_1) \sim_H (E_2, \alpha_2)
\]

if there is an isom \( \phi : E_1 \to E_2 \) and an element \( h \in H \) such that

\[
\alpha_1 = h \circ \alpha_2 \circ \phi \quad \text{(think of } h \in H \text{ as } h : (\mathbb{Z}/N\mathbb{Z})^2 \cong (\mathbb{Z}/N\mathbb{Z})^2)\).

**Exercise.** Let \( H = B_1(N) \). Show that \((E_1, \alpha_1) \sim_H (E_2, \alpha_2)\) if and only if there is an isomorphism \( \phi : E_1 \to E_2 \) such that \( \phi(P_1) = P_2 \), where

\[
P_1 = \alpha_1^{-1}(1, 0), \quad P_2 = \alpha_2^{-1}(1, 0),
\]

are respectively points of order \( N \) on \( E_1, E_2 \).
We want to generalise previous constructions to an arbitrary group $H \leq \text{GL}_2(\mathbb{Z}/N\mathbb{Z})$.

- An isomorphism $\alpha : E[\mathcal{N}] \to (\mathbb{Z}/N\mathbb{Z})^2$ a level $N$ structure on $E$.

- A level $N$-structure is same as choice of basis for $E[\mathcal{N}]$: $P = \alpha^{-1}(e_1)$, $Q = \alpha^{-1}(e_2)$ where $e_1 = (1,0)$, $e_2 = (0,1)$.

- We call pairs $(E_1, \alpha_1)$ and $(E_2, \alpha_2)$ $H$-isomorphic, and write
  $$(E_1, \alpha_1) \sim_H (E_2, \alpha_2)$$
  if there is an isom $\phi : E_1 \to E_2$ and an element $h \in H$ such that
  $$\alpha_1 = h \circ \alpha_2 \circ \phi$$
  (think of $h \in H$ as $h : (\mathbb{Z}/N\mathbb{Z})^2 \cong (\mathbb{Z}/N\mathbb{Z})^2$).

**Exercise.** Let $H = B_0(N)$. Show that $(E_1, \alpha_1) \sim_H (E_2, \alpha_2)$ if and only if there is an isomorphism $\phi : E_1 \to E_2$ such that $\phi(\langle P_1 \rangle) = \langle P_2 \rangle$, where

$$P_1 = \alpha_1^{-1}(1,0), \quad P_2 = \alpha_2^{-1}(1,0),$$

are respectively points of order $N$ on $E_1, E_2$. 
The congruence subgroup associated to $H \leq \text{GL}_2(\mathbb{Z}/N\mathbb{Z})$

Let

$$\Gamma_H := \{ A \in \text{SL}_2(\mathbb{Z}) : (A \mod N) \in \text{SL}_2(\mathbb{Z}/N\mathbb{Z}) \cap H \}.$$  

Then

$$\Gamma_H \supseteq \Gamma(N) := \{ A \in \text{SL}_2(\mathbb{Z}) : A \equiv I \pmod{N} \}.$$  

∴ $\Gamma_H$ is a congruence subgroup of $\text{SL}_2(\mathbb{Z})$.

Exercise. Show that

$$\Gamma_{B_0(N)} = \Gamma_0(N), \quad \Gamma_{B_1(N)} = \Gamma_1(N).$$
The congruence subgroup associated to $H \leq \text{GL}_2(\mathbb{Z}/N\mathbb{Z})$

Let
$$
\Gamma_H := \{ A \in \text{SL}_2(\mathbb{Z}) : (A \mod N) \in \text{SL}_2(\mathbb{Z}/N\mathbb{Z}) \cap H \}.
$$

Given $\tau \in \mathbb{H}$ we write $\alpha_\tau$ for the level $N$ structure on $\mathbb{C}/(\mathbb{Z} + \mathbb{Z}\tau)$:
$$
\alpha_\tau(1/N) = (1,0), \quad \alpha_\tau(\tau/N) = (0,1).
$$

- if $E/\mathbb{C}$, $\alpha$ level $N$-structure on $E$ then
  - there is $\tau \in \mathbb{H}$ such that $E = E_\tau$;
  - the isomorphism $E_\tau(\mathbb{C}) \cong \mathbb{C}/(\mathbb{Z} + \mathbb{Z}\tau)$ identifies $\alpha$ with $\alpha_\tau$;
  - can think of $(E, \alpha)$ as $(\mathbb{C}/(\mathbb{Z} + \mathbb{Z}\tau), \alpha_\tau)$.

- $[(\mathbb{C}/(\mathbb{Z} + \mathbb{Z}\tau_1), \alpha_{\tau_1})]_H = [(\mathbb{C}/(\mathbb{Z} + \mathbb{Z}\tau_2), \alpha_{\tau_2})]_H$ iff $\tau_1 = \gamma(\tau_2)$ for some $\gamma \in \Gamma_H$.

We conclude that there is a one-one correspondence
$$
\Gamma_H \backslash \mathbb{H} \leftrightarrow \{(E/\mathbb{C}, \alpha)]_H\}, \quad \Gamma_H \cdot \tau \mapsto [(\mathbb{C}/(\mathbb{Z} + \mathbb{Z}\tau), \alpha_\tau)]_H.
$$
The modular curve $X_H$

∃ algebraic curves $X_H \supset Y_H$, with $X_H$ complete and $Y_H$ open such that

\[ Y_H(\mathbb{C}) \cong \Gamma_H \backslash \mathbb{H}, \quad X_H(\mathbb{C}) \cong \Gamma_H \backslash \mathbb{H}^*. \]

\[ \text{det}(H) \leq (\mathbb{Z}/N\mathbb{Z})^* \xrightarrow{\chi_N} \text{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \]

Make sense to write

\[ L_H := \mathbb{Q}(\zeta_N)^{\text{det}(H)}. \]

Theorem

The modular curve $X_H$ has a model defined over $L_H$. 
$L_H := \mathbb{Q}(\zeta_N)^{\det(H)}.$

**Theorem**

The modular curve $X_H$ has a model defined over $L_H$.

$\Gamma_H \subset \text{SL}_2(\mathbb{Z}) \quad \implies \quad \exists$ surjective morphism of Riemann surfaces

$$\Gamma_H \backslash \mathbb{H}^* \to \text{SL}_2(\mathbb{Z}) \backslash \mathbb{H}^*, \quad \Gamma_H \cdot \tau \to \text{SL}_2(\mathbb{Z}) \cdot \tau.$$ 

This induces a non-constant morphism of curves

$$j : X_H \to X(1),$$

defined over $L_H$. The **cusps of** $X_H$ is set $j^{-1}(\infty)$, and $Y_H := X_H \backslash j^{-1}(\infty)$.

On complex points it factors through the earlier $j$-map

$$\text{SL}_2(\mathbb{Z}) \backslash \mathbb{H}^* \to X(1)(\mathbb{C}).$$
**Assumption:** Henceforth suppose \( \det(H) = (\mathbb{Z}/N\mathbb{Z})^* \). \( \therefore X_H \) is defined over \( \mathbb{Q} \) (in fact defined over \( \text{Spec}(\mathbb{Z}[1/N]) \)) and so is \( j : X_H \to X(1) \).

Let \( K \) be a perfect field, \( \text{char}(K) = 0 \), or \( \text{char}(K) \nmid N \).

- A point \( Q \in Y_H(\overline{K}) \) represents class \( [(E, \alpha)]_H \) where \( E/\overline{K} \), \( \alpha \) a mod \( N \) level structure;
- we identify \( Q = [(E, \alpha)]_H \).

**Lemma**

Let \( Q = [(E, \alpha)]_H \in Y_H(\overline{K}) \). Let \( E'/\overline{K} \) be an elliptic curve that is isomorphic to \( E \). Then there is some isomorphism \( \alpha' : E'[N] \to (\mathbb{Z}/N\mathbb{Z})^2 \) such that \( Q = [(E', \alpha')]_H \).

i.e. I can replace \( E \) by any isomorphic \( E' \) and obtain the same point \( Q \in Y_H \) provided I suitably choose the mod \( N \) level structure on \( E' \).
Lemma

Let \( Q = [(E, \alpha)]_H \in Y_H(K) \). Let \( E'/K \) be an elliptic curve that is isomorphic to \( E \). Then there is some isomorphism \( \alpha' : E'[N] \to (\mathbb{Z}/N\mathbb{Z})^2 \) such that \( Q = [(E', \alpha')_H] \).

i.e. I can replace \( E \) by any isomorphic \( E' \) and obtain the same point \( Q \in Y_H \) provided I suitably choose the mod \( N \) level structure on \( E' \).

Proof.

Recall \( [(E, \alpha)]_H = [(E', \alpha')_H] \) iff \( \exists \phi : E \to E' \) (isom) and \( h \in H \) such that \( \alpha = h \circ \alpha' \circ \phi \).

Let \( \phi : E \to E' \) be an isomorphism. Let \( \alpha' = \alpha \circ \phi^{-1} \). Observe that \( \alpha = I \circ \alpha' \circ \phi \) where \( I = \) identity of \( H \).

\[ \therefore [(E, \alpha)]_H = [(E', \alpha')_H]. \]
Galois action and rationality

\[ G_K \text{ acts on pairs } (E, \alpha) \quad (E, \alpha)^\sigma := (E^\sigma, \alpha \circ \sigma^{-1}). \]

Action is compatible with action of \( G_K \) on \( Y_H(\overline{K}) \):

\[ Q = [(E, \alpha)]_H \implies Q^\sigma = [(E^\sigma, \alpha \circ \sigma^{-1})]_H. \]

Lemma

Let \( Q \in Y_H(\overline{K}) \). Then \( Q \in Y_H(K) \) iff \( Q = [(E, \alpha)]_H \) for some \( E/K \),
\( \alpha : E[N] \xrightarrow{\sim} (\mathbb{Z}/N\mathbb{Z})^2 \) such that for all \( \sigma \in G_K \), there is an \( \phi_\sigma \in \text{Aut}_{\overline{K}}(E) \) and \( h_\sigma \in H \) satisfying

\[ \alpha = h_\sigma \circ \alpha \circ \sigma^{-1} \circ \phi_\sigma. \quad (1) \]

Proof. \( \iff \) Condition (2) implies \( (E, \alpha) \sim_H (E, \alpha \circ \sigma^{-1}) \). Thus \( Q^\sigma = Q \) for all \( \sigma \in G_K \) and so \( Q \in Y_H(K) \).
$G_K$ acts on pairs $(E, \alpha)$ \quad $(E, \alpha)^\sigma := (E^\sigma, \alpha \circ \sigma^{-1})$.

Action is compatible with action of $G_K$ on $Y_H(K)$:

$$Q = [(E, \alpha)]_H \implies Q^\sigma = [(E^\sigma, \alpha \circ \sigma^{-1})]_H.$$  

**Lemma**

Let $Q \in Y_H(K)$. Then $Q \in Y_H(K)$ iff $Q = [(E, \alpha)]_H$ for some $E/K$, $\alpha : E[N] \xrightarrow{\sim} (\mathbb{Z}/N\mathbb{Z})^2$ such that for all $\sigma \in G_K$, there is an $\phi_\sigma \in \text{Aut}_{\overline{K}}(E)$ and $h_\sigma \in H$ satisfying

$$\alpha = h_\sigma \circ \alpha \circ \sigma^{-1} \circ \phi_\sigma.$$  

(2)

**Proof.** $\implies$ Suppose $Q = [(E', \alpha')]_H \in Y_H(K)$.

Note $E' \cong E'^\sigma$ for all $\sigma \in G_K$. \therefore $j(E') \in K$. \therefore $E' \cong E$ where $E/K$.

By previous lemma $Q = [(E, \alpha)]_H$ for some $\alpha$.

(2) follows $[(E, \alpha \circ \sigma^{-1})] = Q^\sigma = Q = [(E, \alpha)]$.  

$\square$
The case $-I \notin H$

**Theorem**

Suppose $\det(H) = (\mathbb{Z}/N\mathbb{Z})^*$ and $-I \in H$.

(i) Every $Q \in Y_H(K)$ is supported on some $E/K$ (i.e. $\exists E/K$ and $\alpha : E[N] \xrightarrow{\sim} (\mathbb{Z}/N\mathbb{Z})^2$ such that $Q = [(E, \alpha)]_H$.

(ii) If $Q \in Y_H(K)$ and $j(Q) \neq 0, 1728$, then $Q = [(E, \alpha)]_H$ such that $E$ is defined over $K$ and $\overline{\rho}_{E,N}(G_K) \subset H$ (up to conjugation). Conversely, if there is $E$ is defined over $K$ and $\overline{\rho}_{E,N}(G_K) \subset H$ (up to conjugation) then $[(E, \alpha)] \in Y_H(K)$ for a suitable $\alpha$.

(iii) If $Q \in Y_H(K)$ and $j(Q) \neq 0, 1728$, and $Q = [(E, \alpha)]_H$ as above, then $Q = [(E', \alpha')]$ for any quadratic twist $E'/K$ defined over $K$, and for suitable $\alpha'$. 
Theorem

Suppose \( \det(H) = (\mathbb{Z}/N\mathbb{Z})^* \) and \(-I \in H\).

(ii) If \( Q \in Y_H(K) \) and \( j(Q) \neq 0, 1728 \), then \( Q = [(E, \alpha)]_H \) such that \( E \) is defined over \( K \) and \( \overline{\rho}_{E,N}(G_K) \subset H \) (up to conjugation). Conversely, if there is \( E \) is defined over \( K \) and \( \overline{\rho}_{E,N}(G_K) \subset H \) (up to conjugation) then \( [(E, \alpha)] \in Y_H(K) \) for a suitable \( \alpha \).

Some details for (ii). Note that \( j(Q) = j(E) \). As this \( \neq 0, 1728 \), the automorphism group \( \text{Aut}(E) = \{1, -1\} \). Thus \( \phi_{\sigma} = \pm 1 \) and in particular commutes with all other maps. But

\[
\alpha = h_{\sigma} \circ \alpha \circ \sigma^{-1} \circ \phi_{\sigma} \implies \alpha \circ \sigma = (\phi_{\sigma} h_{\sigma}) \circ \alpha.
\]

This can be rewritten as

\[
\overline{\rho}_{E,N}(\sigma) = \phi_{\sigma} h_{\sigma}
\]

once we have taken \( \alpha^{-1}(1, 0), \alpha^{-1}(0, 1) \) as basis for \( E[N] \). Note that \( \phi_{\sigma} h_{\sigma} = \pm h_{\sigma} \in H \). Thus \( \overline{\rho}_{E,N}(G_K) \subset H \) as required.
The case $-I \notin H$

**Theorem**

Suppose $\det(H) = (\mathbb{Z}/N\mathbb{Z})^*$ and $-I \notin H$.

(i) Every $Q \in Y_H(K)$ is supported on some $E/K$ (i.e. $\exists E/K$ and $\alpha : E[N] \cong (\mathbb{Z}/N\mathbb{Z})^2$ such that $Q = [(E, \alpha)]_H$.

(ii) If $Q \in Y_H(K)$ and $j(Q) \neq 0, 1728$, then $Q = [(E, \alpha)]_H$ such that $E$ is defined over $K$ and $\overline{\rho}_{E,N}(G_K) \subset H$ (up to conjugation). Conversely, if there is $E$ is defined over $K$ and $\overline{\rho}_{E,N}(G_K) \subset H$ (up to conjugation) then $[(E, \alpha)] \in Y_H(K)$ for a suitable $\alpha$.

(iii) If $Q \in Y_H(K)$ and $j(Q) \neq 0, 1728$, and $Q = [(E, \alpha)]_H$ as above, then $E$ is unique.
**Theorem**

Suppose \( \det(H) = (\mathbb{Z}/N\mathbb{Z})^* \) and \(-1 \notin H\).

(ii) If \( Q \in Y_H(K) \) and \( j(Q) \neq 0, 1728 \), then \( Q = [(E, \alpha)]_H \) such that \( E \) is defined over \( K \) and \( \bar{\rho}_{E,N}(G_K) \subset H \) (up to conjugation). Conversely, if there is \( E \) is defined over \( K \) and \( \bar{\rho}_{E,N}(G_K) \subset H \) (up to conjugation) then \( [(E, \alpha)] \in Y_H(K) \) for a suitable \( \alpha \).

(iii) If \( Q \in Y_H(K) \) and \( j(Q) \neq 0, 1728 \), and \( Q = [(E, \alpha)]_H \) as above, then \( E \) is unique.

**Some details.** As before \( \phi_\sigma \in \{\pm 1\} \) and \( \bar{\rho}_{E,N}(\sigma) = \phi_\sigma h_\sigma \).

The map \( \psi : \sigma \mapsto \phi_\sigma \) is a quadratic character.

If \( \psi \) is trivial then \( \bar{\rho}_{E,N}(G_K) \subset H \). Otherwise \( \psi \) is a quadratic character, and by Galois theory its kernel fixes a quadratic extension \( K(\sqrt{d}) \) of \( K \).

Now \( \bar{\rho}_{E_d,N} = \psi \cdot \bar{\rho}_{E,N} \), and thus \( \bar{\rho}_{E_d,N}(\sigma) = h_\sigma \in H \).

Replacing \( E \) by \( E_d \) and adjusting the level structure \( \alpha \) gives \( Q = [(E, \alpha)]_H \) with \( E \) defined over \( K \) and \( \bar{\rho}_{E,N}(G_K) \subset H \).