

The result

Then there is a bijection

$$\left\{ \text{ECs } / \mathbb{Q} \text{ up to isogeny} \right\} \xrightarrow{1:1} \left\{ \begin{array}{l} \text{Normalised newforms of} \\ \cdot) \text{ weight } 2 \\ \cdot) \text{ level } \Gamma_0(N), \text{ some } N \geq 1 \\ \cdot) \text{ rational Fourier coeff.} \end{array} \right\}$$

It is given by $E \mapsto f$ if for almost all p ,

$$\text{tr}(\underbrace{F_p}_{\substack{\uparrow \\ \text{absolute Frob} \\ = \text{relative Frobenius} \\ \text{since } \tilde{E}_p / \mathbb{F}_p}} \in \text{End}(\underbrace{\tilde{E}_p}_{\substack{\uparrow \\ \text{Special fiber } \mathbb{F}_p \otimes_{\mathbb{Z}} \tilde{E} \\ \text{of integral model}}})) = \underbrace{p\text{-th Fourier coeff } a_p}_{@} \text{ of } f$$

absolute Frob = relative Frobenius since $\tilde{E}_p / \mathbb{F}_p$.
 Special fiber $\mathbb{F}_p \otimes_{\mathbb{Z}} \tilde{E}$ of integral model
 $\tilde{E} / \mathbb{Z}[B^{-1}]$ $B =$ primes of bad red.

Here $\text{tr}(F_p) = F_p + F_p^* \in \mathbb{Z}$.

@ RHS: f certain function on upper half-plane \mathbb{H} ,

has expression $f(\tau) = \sum_{n \geq 1} a_n \cdot \exp(2\pi i \cdot n \cdot \tau)$

a_n called n -th Fourier coefficient

{ Idea of proof

Consider cohomology of modular curve:

$$\begin{array}{l} \text{étale} \\ \text{cohom} \end{array} \quad H^1(\bar{\mathbb{Q}} \otimes_{\mathbb{Q}} X_K, \bar{\mathbb{Q}}) \\ \text{comparison isom} \longrightarrow \mathbb{Z} \\ \text{Betti cohom} \quad H^1(X_K(\mathbb{C}), \mathbb{C}) \longleftarrow \begin{array}{l} \text{"usual" cohom.} \\ \text{from Topology 1.} \end{array}$$

-) Modularity Thm \Rightarrow Each E "occurs" in étale cohom
-) Hodge Theory / \mathbb{C} \Rightarrow Betti cohom " = " space of modular forms of weight 2, level K

Then consider a huge ring^(*), the Hecke algebra \mathcal{H} .

It acts naturally (compatibly w/ comparison iso)

on both cohom groups, decomposing them into eigenspaces.

Matching eigenspaces by eigenvalues gives bijection from theorem.

(*) \mathcal{H} still very simple, polynomial

$$\text{ring } \mathbb{Q}[T_p, \langle p \rangle^{\pm 1}; p \in K]$$

Modularity Thm

Thm (Wiles, Breuil - Conrad - Diamond - Taylor)

For every EC E/\mathbb{Q} , there is an $N \geq 1$ and a non-constant map $X_{\Gamma_0(N)} \xrightarrow{f} E$.

f called modular parametrization of E

Notation $M_N, M_{N,p} / \mathbb{Z}[\frac{1}{N}]$ usual moduli spaces

$$Y_N, Y_{N,p} := \mathbb{Q} \otimes_{\mathbb{Z}} M_N \text{ resp. } \mathbb{Q} \otimes_{\mathbb{Z}} M_{N,p}$$

(smooth affine curves over $\text{Spec } \mathbb{Q}$.)

$X_N, X_{N,p} :=$ unique smooth compactification
of Y_N resp. $Y_{N,p}$

(Two constructions: 1) Pick $Y \rightarrow \mathbb{P}_{\mathbb{Q}}^1$ non-constant,
put $X :=$ normalization of $\mathbb{P}_{\mathbb{Q}}^1$ in Y .

2) $|X| := \left\{ \text{valuations } v \text{ on } \mathbb{Q}(Y) \text{ s.t. } v|_{\mathbb{Q}} \text{ trivial} \right\} / \sim$

topology: closed sets = $\{v_1, \dots, v_r\}$ v_i non-constant,
 $r < \infty$

$$\mathcal{O}_X(U) = \left\{ f \in \mathbb{Q}(Y) \mid v(f) \geq 0 \ \forall v \in U \right\} .$$

We use as black box that $M_N, M_{N,p}$ have natural smooth compactifications $M_N^*, M_{N,p}^* / \mathbb{Z}[\frac{1}{N}]$.

Let $K \subseteq \mathrm{GL}_2(\hat{\mathbb{Z}})$ any level.

Assume $K \cap \mathrm{GL}_2(\mathbb{Z}_p) = \mathrm{GL}_2(\mathbb{Z}_p)$

Pick N s.t. $K(N) \subseteq K$ and $(p, N) = 1$.

Define $M_K, M_{K,p}, Y_K$, etc. as quotient of $M_N, M_{N,p}, Y_N, \dots$ by $K/K(N)$.

\implies This defines $X_{\Gamma_0(N)} = X_{K_0(N)}$ from Thm.

($X_{\Gamma_0(N)}$ = coarse moduli of $(E, C \subseteq E)$, $C \cong \mathbb{Z}/N$ étale locally.)

Reinterpretation in terms of the Jacobian.

Def $J_K :=$ Jacobian of X_K

$:=$ abelian variety representing $\mathrm{Pic}_{X_K/\mathbb{Q}}^0$.

$\mathrm{Pic}_{X_K/\mathbb{Q}}^0(S) = \{ \mathcal{L} \text{ on } S \times_{\mathrm{Spec} \mathbb{Q}} X_K \text{ s.t.}$

$\deg \mathcal{L}(s)|_C = 0 \quad \forall s \in S, C \in \pi_0(X(S) \otimes X_K) \}$ / $\mathrm{Pic}(S)$

(The defn. captures that X_k might be non-connected.

Note that $X_{\Gamma_0(N)}$ is geometrically connected since

$$\det : \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \in GL_2(\mathbb{Z}/N) \right\} \longrightarrow (\mathbb{Z}/N)^\times$$

is surjective. This is the case of interest,

J is then usual Jacobian.)

Prop (Poincaré reducibility) k any field

$\{ AV/k \text{ w/ } \mathbb{Q} \otimes_{\mathbb{Z}} \text{Hom}(-, -) \}$ (isogeny category of AVs)

is semi-simple.

Idea Given: $Y \hookrightarrow X$ sub-AV. Pick

ample l.b. \mathcal{L} on X , consider induced polarization

$$\phi_{\mathcal{L}} : X \longrightarrow X^\vee. \quad \text{Put } Z = \ker(X^\vee \longrightarrow Y^\vee).$$

Then one may show that $Y \times \phi_{\mathcal{L}}^{-1}(Z) \longrightarrow X$

is an isogeny. (cf. AV Lect 25 or Mumford §19 Thm 1) \square

$$\Rightarrow J_K \underset{\exists \text{ isogeny}}{\sim} \prod_{i=1}^r A_i^{n_i}$$

for uniquely determined $n_i \geq 1$ and simple abelian varieties with $\text{Hom}(A_i, A_j) = 0$ $i \neq j$.

A simple $\stackrel{\text{def}}{=} Z \subseteq A$ sub-AV $\Rightarrow Z = 0$ or A .
 $\Leftrightarrow \text{End}^0(A)$ is a division algebra.

Prop. There always exist finite morphisms $X \rightarrow J$:

E.g. assume X connected, let $D \in \text{Div}(X)$ any s.d.

$\deg D \neq 0$. Then $x \mapsto \mathcal{O}(D - \deg(D) \cdot [x])$

defines such a map. In this case, the composition

$$X^g \rightarrow J^g \xrightarrow{\Sigma} J \quad g = \text{genus of } X$$

is surjective & generically finite.

It follows that, for an AV A :

$$\exists \text{ non-constant } X \rightarrow A \quad (\Leftrightarrow) \quad \exists J \xrightarrow{\neq 0} A$$

$$(\Leftrightarrow) A \sim A_i \text{ for some } i$$

Example ECs are simple since of dimension 1.

There is a moduli space $\mathcal{A}_g/\mathcal{O}$ of principally polarized AVs of dim g . It has $\dim \mathcal{A}_g = \frac{g(g+1)}{2}$.

In particular,

$$\dim \mathcal{A}_h \times \mathcal{A}_{g-h} < \dim \mathcal{A}_g \quad \forall 0 < h < g.$$

\Rightarrow "Most" AVs/ \mathcal{O} are not products of smaller - dim

AVs up to isogeny, meaning they are simple.

Reformulation of Modularity Theorem:

Every EC E/\mathbb{Q} occurs in some $J_0(N)$.

Correspondences

Why bother?

G group, $G \curvearrowright X$, $K \subseteq G$ subgroup.

Then no G -action on $K \backslash X$ anymore!

Namely $Kx_1 = Kx_2$ does not imply

$Kgx_1 = Kgx_2$ in general.

Only the set of all possible choices is well-defined:

$$g \cdot x := K \backslash KgKx \subseteq K \backslash X$$

i.e. new $g \cdot$ - as multivalued map (= correspondence)

$$C_g := \left\{ (Kx_1, Kx_2) \mid \exists k_1, k_2 \text{ s.t. } gk_1x_1 = k_2x_2 \right\}$$

$$\Leftrightarrow k_2^{-1}gk_1 \cdot x_1 = x_2$$

Now let $V =$ functions on X

(or sections of a G -equivariant bundle)

Then $G \curvearrowright V$ by translation and

K -invariants $V^K =$ functions on $K \backslash X$

But V^k not G -stable in general, only

$$g \cdot v \in V^{gkg^{-1}} \text{ if } v \in V^k$$

Assume however that $K \backslash KgK$ is finite, so

$$p_1 : C_g \rightarrow K \backslash X \text{ is finite.}$$

Then can define

$$C_g : V^k \rightarrow V^k, f \mapsto p_{1,*} (p_{2|C_2}^* f)$$

take fiber-wise sum

$$\text{rep. } v \mapsto \sum_{i \in I} h_i \cdot v \quad \underline{K\text{-averaging}}$$

where $KgK = \bigsqcup_{i \in I} K \cdot h_i$ (I finite by assump.)

Our case of interest: $G = GL_2$

$$G(\mathbb{Q}) \backslash (\mathbb{H}^\pm \times G(\mathbb{A}_f)) \supset G(\mathbb{A}_f)$$

\cup

K level subgroup.

Def X smooth proper curve / k

$\text{Corr}(X) := \mathcal{A}$ -vsp generated by

closed integral $Z \subseteq X \times X$ s.th.

$p_1, p_2: Z \rightarrow X$ are finite loc free

(As X smooth, this is equivalent to $\dim Z = 1$

and $p_1, p_2|_Z$ non-constant.)

Becomes a ring (\mathcal{A} -algebra) under

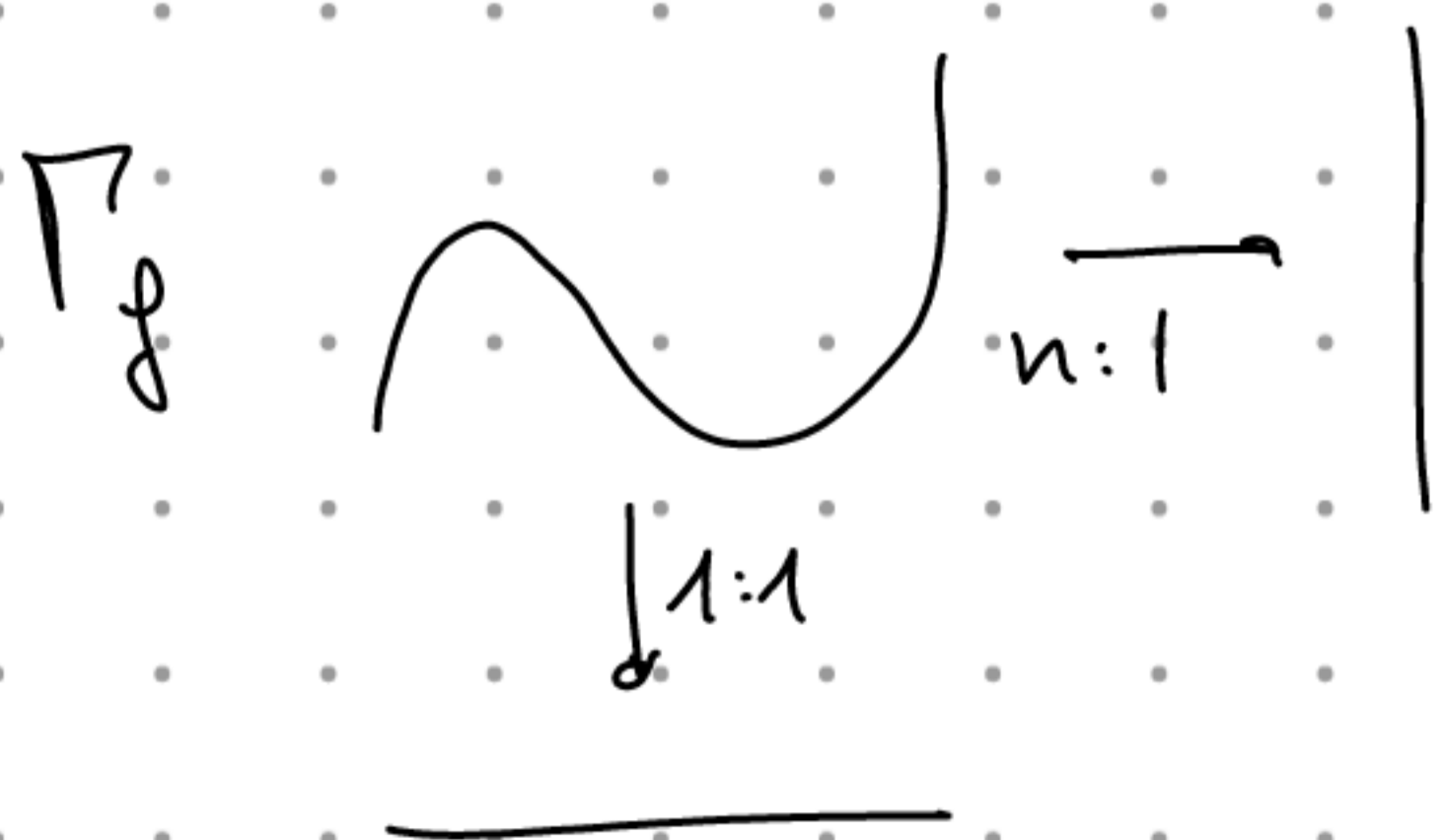
$$Z_1 * Z_2 := \text{Im} \left(Z_1 \times_{p_2, X, p_1} Z_2 \xrightarrow{(p_1, p_2)} X \times X \right)$$

In following sense: $Z_1 \times Z_2 = \bigcup_{i=1}^r Y_i$ irred components.

Then $\text{RHS} = \sum [k(Y_i) : k(p(Y_i))] \cdot p(Y_i)$

$$p = (p_1, p_2)$$

Example $f: X \rightarrow X$ non-constant has graph



Check $\Gamma_f * \Gamma_g = \Gamma_{g \circ f}$

So correspondences generalise
concept of maps!

There is a ring morphism $\text{Corr}(X) \rightarrow \text{End}^0(\mathbb{J})$:

$$Z^* \mathcal{L} := \det(p_{1,*}(p_2^* \mathcal{L})) \otimes \det(p_{1,*} \mathcal{O}_Z)^{-1}$$

line bundle on $S \times_k X$

(Here one has to put $\det \mathcal{O} := \mathcal{O}_X$ to cover $Z=0$.)

Concretely for $S = \text{Spec } k$:

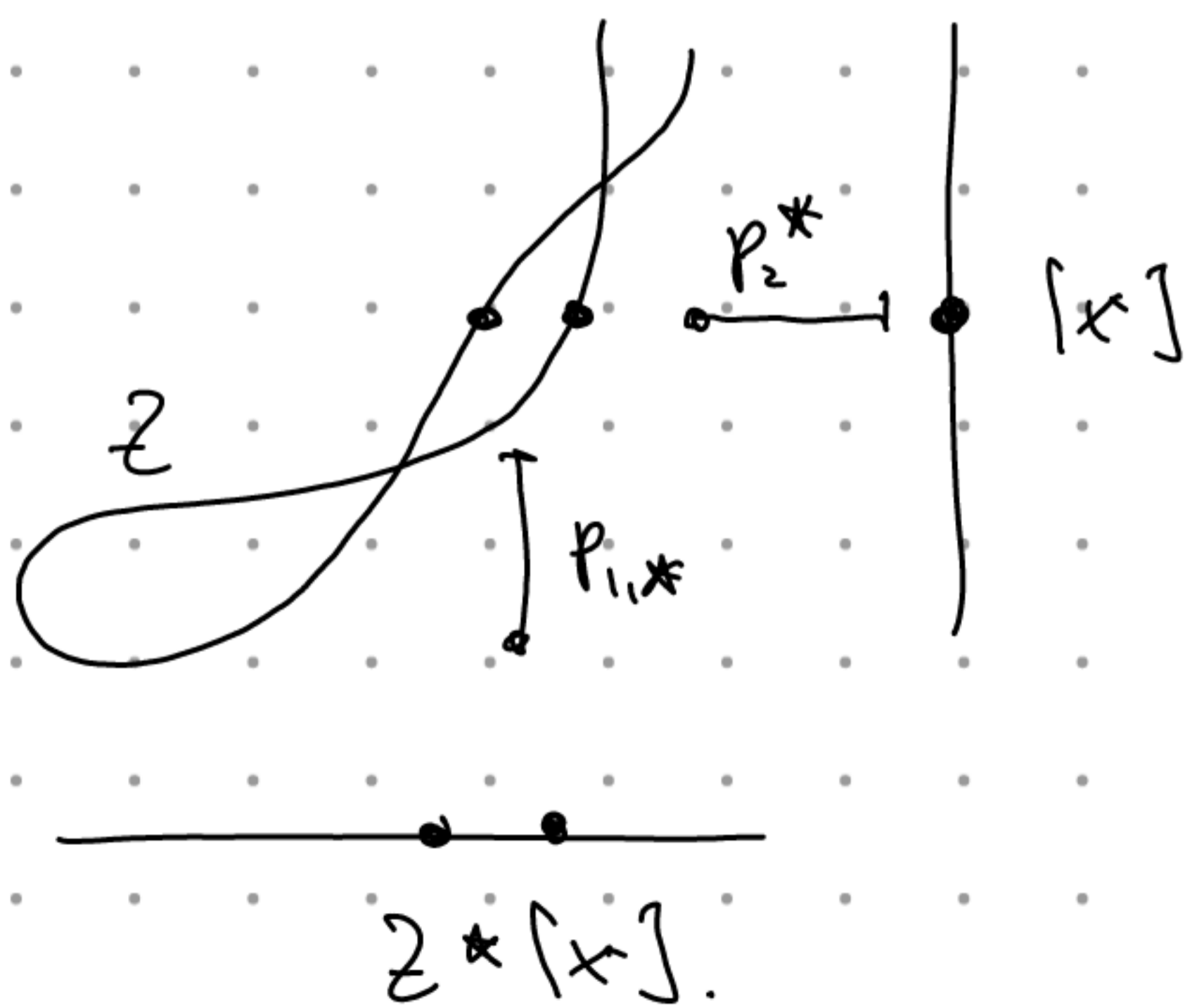
Consider $\mathcal{L} = \mathcal{O}_X([x])$ w/ $p_2^{-1}(x) \subseteq$ normal locus of Z .

$$\text{Then } p_2^* \mathcal{L} = \mathcal{O}_Z \left(\sum_{p_2(z)=x} e_{p_2,z} \cdot [z] \right)$$

$$\text{and } v_{x^1}(\det p_{1,*} \mathcal{O}_Z \rightarrow \det p_{1,*} p_2^* \mathcal{L})$$

$$= \sum_{\substack{p_1(z)=x^1 \\ p_2(z)=x}} e_{p_1,z} \cdot \delta_{p_1,z} \cdot e_{p_2,z} \cdot [x^1]$$

$\Rightarrow Z^*$ - comes from the multi-valued map defined by Z .



From divisor description we see that

$$\deg \mathcal{L} = 0 \implies \deg \tau_* \mathcal{L} = 0,$$

so get map $\mathcal{J} \rightarrow \mathcal{J}$ as claimed.

(Exercise: Check from divisor description that

$$\tau_1 * (\tau_2 * \mathcal{L}) = (\tau_1 * \tau_2) * \mathcal{L}.)$$

See Fulton §16 for more details.

Hecke correspondence

Let p prime, $K = \mathrm{GL}_2(\mathbb{Z}_p) \subseteq \mathrm{GL}_2(\mathbb{Q}_p)$

Def Hecke algebra $\mathcal{H}_p \stackrel{\text{def}}{=} \mathbb{Q}[\mathrm{GL}_2(\mathbb{Z}_p) \backslash \mathrm{GL}_2(\mathbb{Q}_p) / \mathrm{GL}_2(\mathbb{Z}_p)]$
(finite linear combinations of double cosets.)

view as left and right K -invariant functions with

compact support on $\mathrm{GL}_2(\mathbb{Q}_p)$. Then multiplication is

convolution

$$(f * g)(x) = \int_{\mathrm{GL}_2(\mathbb{Q}_p)} f(y) g(y^{-1}x) dy$$

w.r.t. unique translation invariant measure s.t. $\mu(K) = 1$.

Elementary divisors then:

$$K \backslash GL_2(\mathbb{Q}_p) / K = \left\{ K \cdot \begin{pmatrix} p^a & \\ & p^b \end{pmatrix} K \mid a \geq b \right\}$$

$\Rightarrow \coprod K \begin{pmatrix} p^a & \\ & p^b \end{pmatrix} K$ form a-basis for \mathcal{H}_p .

$$\begin{aligned} \begin{pmatrix} p & \\ & p \end{pmatrix} \text{ lies in center, so } K \begin{pmatrix} p & \\ & p \end{pmatrix} K \\ = K \begin{pmatrix} p & \\ & p \end{pmatrix} = \begin{pmatrix} p & \\ & p \end{pmatrix} K \end{aligned}$$

Put $\langle p \rangle := \coprod K \begin{pmatrix} p & \\ & p \end{pmatrix} K$. Then

$$\langle p \rangle * \coprod K \begin{pmatrix} p^a & \\ & p^b \end{pmatrix} K = \coprod K \begin{pmatrix} p^{a+1} & \\ & p^{b+1} \end{pmatrix} K.$$

What about $T_{p^i} := \coprod K \begin{pmatrix} p^i & \\ & 1 \end{pmatrix} K$?

Have following description: $GL_2(\mathbb{Q}_p) / GL_2(\mathbb{Z}_p) \cong \left\{ \Lambda \subseteq \mathbb{Q}_p^2 \right\}$
lattices

So $\mathcal{H}_p = \text{Map}_c(\{\Lambda\}, \mathbb{Q})$
finite support $\xrightarrow{GL_2(\mathbb{Z}_p)}$ invariant under $GL_2(\mathbb{Z}_p)$ -action on $\{\Lambda\}$.

Multivalued map $T_{p^i}(\Lambda) = \left\{ \Lambda' \subseteq \Lambda, \Lambda / \Lambda' \cong \mathbb{Z}/p^i \right\}$
 \longleftarrow elementary divisor $(p^i, 1)$.

$$\left(\text{Rmk } \# T_{pi}(\lambda) = \# P'(\mathbb{Z}/p^i) = p^{i-1}(p+1) \right)$$

Then $T_{pi} \subset \text{Map}_c(\{\lambda\}, \mathbb{Q})$ via

$$T_{pi} \left(\sum_r \lambda_r \mathbb{1}_{\lambda_r} \right) = \sum_r \lambda_r \mathbb{1}_{T_{pi}(\lambda_r)}$$

and thus describes multiplication in \mathcal{H}_p !

$$\Rightarrow T_p * T_p = T_{p^2} + (p+1) \langle p \rangle$$

$$= \sum_{\substack{\lambda' \subset \lambda \subset \mathbb{Z}_p^2 \\ \lambda' \subset \lambda \subset \mathbb{Z}_p^2}} \mathbb{1}_{\lambda'}$$

For $\lambda' = p \cdot \mathbb{Z}_p^2$,

there are $p+1$ ways to squeeze $\lambda' \subset \lambda \subset \mathbb{Z}_p^2$

If $\mathbb{Z}_p^2 / \lambda' \cong \mathbb{Z}/p^2$, there

is a unique squeezed

$$\lambda' \subset \lambda \subset \mathbb{Z}_p^2$$

Such arguments show:

$$\text{Prop } \mathcal{H}_p = \mathbb{Q}[\langle p \rangle^{\pm 1}, T_p]$$

$$\left(\cong \mathbb{Q}[S^{\pm 1}, T] \text{ commutative polynomial ring!} \right)$$

Now back to global setting, $N \geq 1$. One obtains

$$\bigotimes_{p+N} \mathcal{H}_p \longrightarrow \text{Conn}(X_N)$$

$$\cdot) \quad \langle p \rangle \longmapsto \langle p \rangle \text{ operator}$$

$$\langle p \rangle (E, \alpha) = (E, p\alpha) \text{ on } Y_K$$

View as correspondence via graph $\Gamma_{\langle p \rangle}$.

$$\cdot) \quad T_p \longmapsto X_{N,p}$$

View $X_{N,p}$ as correspondence via the two maps

$$(E, \alpha, C) \longmapsto ((E, \alpha), (E/C, \alpha \bmod C))$$

(The multivalued map is thus $[E] \longmapsto \sum_{\substack{E \rightarrow E' \\ \text{of deg } p}} [E']$.)

Upshot Let $K(N) \subseteq K \in \text{Gal}_2(\widehat{\mathbb{Z}})$ level, e.g. $K_0(N)$.

$$\text{Obtain } \mathcal{Q}[\langle p \rangle^{\pm 1}, T_p; p+N] \longrightarrow \text{End}^0(J_K)$$

$$\mathcal{H}^N := \bigotimes_{p+N} \mathcal{H}_p$$

Hecke algebra away from N

Recall May write $J_K \sim \prod_{i \in I} A_i^{n_i}$

in unique way with A_i simple, $A_i \not\sim A_j$ $i \neq j$.

Then $\text{End}^0(J_K) = \prod_{i \in I} M_{n_i}(D_i)$ $D_i = \text{End}^0(A_i)$
division \mathbb{Q} -algebra.

Contains the projections $e_i = (0, \dots, 0, 1_i, 0, \dots, 0)$

Thm 1) The image of $\mathcal{H}^N \rightarrow \text{End}^0(J_K)$

contains the idempotents e_i .

2) Given an EC E/\mathbb{Q} , there exists a choice of

level K s.th. $J_K \sim E \times A$

with $\text{Hom}(E, A) = 0$. (Newform theory)
+ modularity thm.

Remark This theorem is proved analytically by studying

1 modular forms, ie. $H_{\text{Betti}}^1(X_K(\mathbb{C}), \mathbb{C})$,

and then carries over through the comparison

iso with étale cohomology.

Eichler - Shimura

K s.th. $J_K \sim E \times A$, $\text{Hom}(E, A) = 0$.

Question What is the composition

$$\mathbb{H}^N \rightarrow \text{End}^0(J_K) \xrightarrow{\text{pr}} \text{End}^0(E)$$

$$T_p \xrightarrow{\quad\quad\quad} ?$$

(E occurs for $K_0(N)$ and any subgroup $C \subseteq E$

\Rightarrow stable under p , so one knows a priori that

$\langle p \rangle \mapsto \text{id}_E$. The $\langle p \rangle$ -operator only plays a

role when refining the level, e.g. $\Gamma_1(N) \mapsto K_1(N)$.)

Then $T_p \mapsto a_p \in \mathbb{Z} \subseteq \text{End}^0(E)$,

$$a_p = \text{tr}(F_p) = F_p + F_p^* = F_p + V_p = p+1 - \chi \tilde{E}(F_p)$$

(This is the corrected sign)

Proof: $M_K / \mathbb{Z}[\frac{1}{N}]$ has a smooth compactification M_K^*

(Means $M_K^* \rightarrow \text{Spec } \mathbb{Z}[\frac{1}{N}]$ proper smooth, contains

M_K as dense open.)

$\Rightarrow J_K$ extends to abelian scheme over $\mathbb{Z}[\frac{1}{N}]$.

namely $\tilde{J}_K := \text{Pic}^0_{M_K^*} / [2\frac{1}{N}]$.

.) Weil extension Thm:

$$\text{End}(J_K) = \text{End}(\tilde{J}_K)$$

In pic , the idempotent $(E \times A \xrightarrow{\text{pr}} E \xrightarrow{\text{inc}} E \times A)$

lifts to \tilde{J}_K , giving $\tilde{J}_K \sim \tilde{E} \times \tilde{A}$

In pic , E also has good reduction, model \tilde{E} .

.) Furthermore, (a compactification of) $M_{K,p}$

provides an integral model of T_p that describes

the image of $T_{p, \mathcal{O}}$ under Weil extension

$$\text{End}(J_K) \xrightarrow{\cong} \text{End}(\tilde{J}_K)$$

$$\& \text{End}(E) \xrightarrow{\cong} \text{End}(\tilde{E})$$

.) By rigidity, $\text{End}(\tilde{J}_K) \hookrightarrow \text{End}(\#_l \otimes \tilde{J}_K)$

$$\text{End}(\tilde{E}) \hookrightarrow \text{End}(\#_l \otimes \tilde{E})$$

for any prime $l \neq N$.

We choose to work at the "bad" (= interesting) prime $l=p$.

·) $\#_p \otimes \tilde{J}_K =$ Jacobian of special fib \overline{M}_K^*

& interact here with its endomorphism defined by special fibres of correspondence $\overline{M}_{K,p}^*$

(This just expresses functoriality properties of the Jacobian construction and the map $\text{Corr}(X) \rightarrow \text{End}(J)$.)

·) In $\text{Corr}(\overline{M}_K^*)$, $\mathbb{F} \quad \mathbb{V}$
 $\overline{M}_{K,p}^* = \mathbb{I}(\overline{M}_K^*) \perp \omega \mathbb{I}(\overline{M}_K^*)$

Identifying them with \overline{M}_K^* via \mathbb{I} and $\omega \mathbb{I}$,

there are

$$\mathbb{I} : \begin{array}{ccc} \overline{M}_K^* & \xrightarrow{\text{Frob}} & \overline{M}_K^* \\ \downarrow \text{id} & & \\ \overline{M}_K^* & & \end{array} \quad \omega \mathbb{I} : \begin{array}{ccc} \overline{M}_K^* & \xrightarrow{\langle p \rangle} & \overline{M}_K^* \\ \downarrow \text{Frob} & & \\ \overline{M}_K^* & & \end{array}$$

The composition F^*V in $\text{Corr}(\overline{M}_K^*)$ acts
on \tilde{T}_p (in terms of divisors) as

$$D \mapsto \text{Frob}^* \text{Frob}_* \langle p \rangle^* D = p \cdot \langle p \rangle^* D.$$

(Given $f: X \rightarrow Y$ degree d map of curves,
 $f_* f^* D = d \cdot D$)

F itself acts as Verschiebung of \tilde{T}_p by functoriality.

$$\Rightarrow V = \langle p \rangle \cdot F^* \quad \text{dual isogeny.}$$

.) Mentioned above: $\langle p \rangle \mapsto 1$ in $\text{End}(\tilde{E})$

$$\Rightarrow T_p \mapsto F + F^* = \text{tr}(F) \in \text{End}(E)$$



On the other hand \exists 1-dimensional \mathbb{H}^N -stable summand

$$\mathbb{C} \cdot \mathcal{I}_E \subseteq \{ \text{Modular forms of wt } 2, \text{ level } K \}$$

that corresponds to E under comparison iso étale \rightarrow Betti.

Thus $T_p \subset \mathbb{C} \cdot \mathcal{I}_E$ also via a_p !

If δ_E is normalized, then this reflects in its

Fourier coeff. being a_p .