COMPUTATIONAL ASPECTS OF SHIMURA CURVES

Drew Sutherland
John Voight

BB4
Budapest
July 2018

§ Elliptic curves

1) Smooth projective curve of genus 1 with distinguished rational point (E, O).
Group law, Weierstrass equation...

2) Abelian variety of dimension 1, projective algebraic group.

Jacobians X/k "smooth projective curve of genus g, geometrically irreducible" = nice

$$\left\{ \begin{array}{l} X/k \text{ nice curve} \\ \text{of genus } g \end{array} \right\} \xrightarrow[\text{Jac}]{} \left\{ \begin{array}{l} \text{abelian variety of dim } g \\ \text{over } k \end{array} \right\}.$$

Closed point: $\mathrm{Gal}(\bar{k}/k)$-orbit of $X(\bar{k})$.

$\mathrm{Div}(X) = \mathbb{Z}[P : P \text{ closed point}]$ $\quad D = \sum n_P P$.

$\deg(P) = \# P$; $\quad \deg(D) = \sum n_P \deg(P)$.

Coordinate ring $k[X] = k[x_1, \ldots, x_n]/(I(X))$; function field $k(X) = \mathrm{Frac}\, k[X]$.

$$\left\{ \begin{array}{l} \text{smooth projective} \\ \text{curves over } k \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{l} \text{function fields } k(X) \\ \text{i.e. finite extensions } k(X) \ (\mathrm{trdeg} = 1) \end{array} \right\}.$$

$f \in k(X) \rightsquigarrow \mathrm{div}(f) = \sum \mathrm{ord}_P(f) P$. $\quad \deg(\mathrm{div}(f)) = 0$.

$\mathrm{Div}^0 X = \{ D \in \mathrm{Div}(X) : \deg D = 0 \}$ $\qquad \mathrm{Pic}^0 X = \dfrac{\mathrm{Div}^0 X}{\mathrm{Princ}\, X}$.

$\mathrm{Princ}\, X = \{ \mathrm{div}\, f : f \in k(X) \}$.

If $X(k) \neq \emptyset$ then $\mathrm{Pic}^0 X \cong \mathrm{Jac}(X)$.

- Abel-Jacobi map: $X \to \mathrm{Jac}\, X \cong \mathrm{Pic}^0 X$
$\qquad P \mapsto [P - O]$

If E is an elliptic curve, then this is an isomorphism.

Now suppose that $k = \mathbb{Q}$ (or a # field embedded in $\mathbb{C}$)

A/k ab. var of dim g $\Rightarrow A(\mathbb{C})$ is a compact Lie group
$\cong \mathbb{C}^g / \Lambda$, $\Lambda \cong \mathbb{Z}^{2g}$. (torus).

Def: $X = V/\Lambda$, $V \cong \mathbb{C}^g$, $\Lambda \cong \mathbb{Z}^{2g}$. Dual torus $X^\vee = V^*/\Lambda^*$,

where $V^* := \{ f : V \to \mathbb{C} : f(\alpha v) = \bar{\alpha} f(v) ; f(v_1 + v_2) = f(v_1) + f(v_2) \}$.

$\Lambda^* := \{ f \in V^* : \mathrm{Im}(f(\Lambda)) \subseteq \mathbb{Z} \}$.

A polarization of X is a positive-definite Hermitian form $H : V \times V \to \mathbb{C}$, s.t.

$\mathrm{Im}\, H(\Lambda, \Lambda) \subseteq \mathbb{Z}$; it induces an isogeny (surjective morphism w/ finite kernel)

$\phi_H : X \to X^\vee$.

A polarization of an abelian variety A/K is an isogeny $\phi : A \to A^\vee$

$v\Lambda \mapsto (w \mapsto H(v,w).\Lambda^*)$

$\left\{ \begin{matrix} \text{polarized abelian} \\ \text{varieties over } \mathbb{C} \end{matrix} \right\} \leftrightarrow \left\{ \begin{matrix} \text{polarized} \\ \text{tori} \end{matrix} \right\}$.

A polarization of degree 1 is called a principal polarization.

Key fact: Jacobians are principally polarized abelian varieties.

§ Endomorphism rings and algebras.

$\mathrm{End}(A) :=$ ring of endomorphisms of A.

$\cup\!\!\shortmid$
$\mathbb{Z}$ since we have multiplication-by-m maps. $[m] : A \to A$.

NB: By $\mathrm{End}(A)$ we mean endomorphisms defined over K

We will also write $\mathrm{End}^0(A) := \mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$, a $\mathbb{Q}$-algebra of finite dimension.

$\phi : A \to A^\vee$ a polarization, $\phi^{-1} \in \mathrm{Hom}(A^\vee, A) \otimes_{\mathbb{Z}} \mathbb{Q}$.

Rosati involution: $\alpha^\dagger := \phi^{-1} \circ \alpha^\vee \circ \phi$

Positive definite: $\mathrm{Tr}_{\mathrm{End}^0 E / \mathbb{Q}} (\alpha \alpha^\dagger) > 0 \quad \forall \alpha \in \mathrm{End}^0 E \setminus \{0\}$.

Let A be a simple abelian variety. (not a product of smaller-dimension ab. vars).

$D := \mathrm{End}^0(A_{\bar{K}})$ is a division algebra $/\mathbb{Q}$. Let $F =$ center of D (a # field)

Let $F^0 := F^\dagger =$ subfield fixed by Rosati.

Then $[D : F] = d^2$ for some $d \in \mathbb{Z}_{>0}$, $e_0 := [F : F^0] = 1, 2$; F^0 totally real.

$e = [F : \mathbb{Q}]$.

ALFRÉD RÉNYI INSTITUTE OF MATHEMATICS · HUNGARIAN ACADEMY OF SCIENCES
13-15 Reáltanoda u, H-1053 Budapest, Hungary | phone: +36 1 483 8300 | fax: +36 1 483 8333 | math@renyi.mta.hu | www.renyi.hu

Thm (Albert).

Assume char $k=0$. Then there are 4 types:

		e_0	d	$D\otimes_{\mathbb{Q}}\mathbb{R}$	constraint
I:	$D=F=F^\circ$	1	1	$\mathbb{R}^e$	$e\mid g$
II:	$F=F^\circ$	1	2	$M_2(\mathbb{R})^e$	$2e\mid g$.
III:	$F=F^\circ$	1	2	$\mathbb{H}^e$	$2e\mid g$
IV:	$F\neq F^\circ$	2	*	$M_d(\mathbb{C})^{e/2}$	$\frac{1}{2}ed^2\mid g$.

Cor ($g=1$): Either:

$\to$ I $\quad\mathbb{R}$

$\to$ IV $\quad\mathbb{C}$

Cor ($g=2$):

$\to$ I $\quad \mathbb{R}$ or $\mathbb{R}^2$ $\swarrow$ RM $\quad$ (3 and 2) $\quad$ (numbers indicate dim of the moduli space).

$\to$ II $\quad M_2(\mathbb{R})$ $\swarrow$ QM $\quad$ (1)

$\to$ III $\quad \mathbb{H}$ $\leftarrow$ this never arises, and it doesn't happen either in odd g.

$\to$ IV $\quad M_2(\mathbb{C})$ $\nwarrow$ CM $\quad$ (0)

§ Torsion subgroups

A/k of dimension g; $A[n]:=\{P\in A(\bar{k}) : nP=0\}$.

$\operatorname{char}(k)\nmid n \Rightarrow A[n]\cong(\mathbb{Z}/n\mathbb{Z})^{2g}$ (easy to see in char 0).

n-torsion field: $k(A[n]) :=$ minimal extension L/k s.t. $A[n]=A(L)[n]$.
(L/k is Galois).

Weil pairing: $e_n : A[n]\times A^\vee[n]\to\mu_n(\bar{k})$ bilinear, non-degenerate, "skew-symmetric" & Galois equivariant.

Given a polarization, can think of it as $e_n : A[n]\times A[n]\to\mu_n(\bar{k})$.

If P is a point of order n,

$$\{Q\in A[n] : e_n(P,Q)=1\}\cong(\mathbb{Z}/n\mathbb{Z})^{g}.$$

ALFRÉD RÉNYI INSTITUTE OF MATHEMATICS · HUNGARIAN ACADEMY OF SCIENCES
13 - 15 Reáltanoda u, H-1053 Budapest, Hungary | phone: +36 1 483 8300 | fax: +36 1 483 8333 | math@renyi.mta.hu | www.renyi.hu

Mordell-Weil: if A is an abelian variety over a # field K, then $A(K)$ is a finitely-generated abelian group. $\cong \mathbb{Z}^r \oplus A(K)_{tor}$ ← finite.

Hyperelliptic curves: a degree-2 cover of $\mathbb{P}^1$.

Assume $char(K) \neq 2$. $\to y^2 = f(x)$ $g(C) = \lfloor \frac{\deg f - 1}{2} \rfloor$.

We'll take f of odd degree, and $g(C) \geq 2$. (elliptic curves get singled-out).

$f(x)$ squarefree $\Rightarrow$ C smooth. (char 2: $y^2 + h(x)y = f(x)$, $\deg h \leq g$).

Hyperelliptic involution: $\overset{(x,y)}{P} \mapsto \overline{P} = (x,-y)$. $\exists!$ point at ∞, call it ∞.

A divisor $D = \sum n_P P$ is effective if $n_P \geq 0$. It can be written as $P_1 + \dots + P_n$ (with repetition).

An effective divisor is semi-reduced if $P_i \neq \overline{P_j}$ $\forall i \neq j$.

If D is semi-reduced and $\deg D \leq g$, then D is reduced.

Def D is affine if it has no points at ∞.

Thm (Mumford): Every divisor class in $\mathrm{Pic}^0(C)$ can be uniquely represented by $[D - n\infty]$ where D is a reduced rational affine divisor.

Mumford's representation:

$D = P_1 + \dots + P_n$ a semi-reduced affine divisor.

$u(x) = \prod (x - x_i) \in K[x]$ monic, squarefree. $P_i = (x_i, y_i) \in C(\overline{K})$.

let $v \in K[x]$ satisfy $\deg v < \deg u$ s.t. $v(x_i) = y_i$.

Then $D = [u, v]$, $u \mid v^2 - f$.

Using extended euclidean algorithm, can use this to implement the group law!

eg: $-[u,v] = [u,-v]$.

Consequence: 2-torsion points in $\mathrm{Jac}(X) \simeq \mathrm{Pic}^0(X)$ have Mumford rep. $[u, 0]$.

ALFRÉD RÉNYI INSTITUTE OF MATHEMATICS · HUNGARIAN ACADEMY OF SCIENCES
13 – 15 Reáltanoda u, H-1053 Budapest, Hungary | phone: +36 1 483 8300 | fax: +36 1 483 8333 | math@renyi.mta.hu | www.renyi.hu

Goal: ~~modular~~ curves parametrize elliptic ~~curves~~ with level structure.
Shimura — abelian surfaces with potential quaternionic multiplication (PQM).

There is a bijection

$$(P)SL_2(\mathbb{Z})\backslash\mathfrak{h} \longleftrightarrow \{\text{elliptic curves over } \mathbb{R}\}/\cong$$

$$SL_2(\mathbb{Z})\cdot\tau \longmapsto \left[\mathbb{C}/\mathbb{Z}\tau+\mathbb{Z}\right] =: [E_\tau].$$

$$\downarrow j$$

$$\mathbb{A}^1(\mathbb{C}) = \mathbb{C}$$

$$\{j \in F\} \longleftrightarrow \{\text{elliptic curves over } F\}/\cong_{F^{alg}}$$

Can add level structure:

$$\Gamma_0(N)\backslash\mathfrak{h} \longleftrightarrow \{(E, C) : C \le E[N],\ C \cong \mathbb{Z}/N\mathbb{Z}\}/\cong$$

$$\Gamma_0(N)\cdot\tau \longmapsto [(E_\tau, \langle \tfrac{1}{N}\rangle)].$$

$\Gamma_0(N) = \left\{\begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \bmod N\right\}$, $\Gamma_1(N) = \left\{\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \bmod N\right\}$ $\subseteq SL_2(\mathbb{Z})$.

Let F be a field, char $F \neq 2$. Let $B := \left(\frac{a,b}{F}\right) := F \oplus Fi \oplus Fj \oplus Fij$

$i^2 = a$, $j^2 = b$, $ij = -ji$.

QUATALG over F.

Example: $\left(\frac{1,1}{F}\right) = M_2(F)$ $\quad \left(\frac{-1,-1}{\mathbb{R}}\right) = \mathbb{H} \not\cong M_2(\mathbb{R})$.

Standard involution: $\bar{\ } : B \to B$, $\alpha \mapsto \bar\alpha$, $\alpha = t + xi + yj + zij \mapsto t - xi - yj - zij$.

$\mathrm{trd}: B \to F$, $\alpha \mapsto \alpha + \bar\alpha$ $\quad$ $\mathrm{nrd}: B \to F$, $\alpha \mapsto \alpha\bar\alpha$. (reduced trace & norm)

Over $\mathbb{Q}_v = \begin{cases} \mathbb{R} \\ \mathbb{Q}_p \end{cases}$, there is a unique division quaternion algebra (up to $\cong$).

Say $B/\mathbb{Q}$ is ramified at $v \in Pl(\mathbb{Q})$ if $B_v := B \otimes_{\mathbb{Q}} \mathbb{Q}_v$ is a division algebra.

$\mathrm{Ram}(B) = \{v \in Pl(\mathbb{Q}) : B \text{ is ramified}\}$ finite & even $\quad$ $\mathrm{disc}(B) = \prod_{p \in \mathrm{Ram}(B)\setminus\{\infty\}} p$.

Thm (classification): The map:

$$\{\text{quaternion alg.}/\mathbb{Q}\}/\cong \xrightarrow{\mathrm{disc}} \{\text{squarefree positive integers}\}.$$

ALFRÉD RÉNYI INSTITUTE OF MATHEMATICS · HUNGARIAN ACADEMY OF SCIENCES
13-15 Reáltanoda u, H-1053 Budapest, Hungary | phone: +36 1 483 8300 | fax: +36 1 483 8333 | math@renyi.mta.hu | www.renyi.hu

Main example: $B = \left(\frac{-1,3}{\mathbb{Q}}\right)$ $\mathrm{Ram}(B) = \{2,3,\cancel{\infty}\}$

$B\otimes\mathbb{R} = \left(\frac{-1,3}{\mathbb{R}}\right) \simeq \left(\frac{1,1}{\mathbb{R}}\right) \simeq M_2(\mathbb{R})$.

$\Rightarrow \mathrm{disc}(B) = 6$.

$B\otimes\mathbb{Q}_3 \simeq M_2(\mathbb{Q}_3)$ because $\left(\frac{-1}{3}\right) = -1$.

Rough overview

$$\begin{array}{ccc} M_2(\mathbb{Q}) & & B \text{ quat. alg } /\mathbb{Q} \text{ (indefinite)} \Rightarrow B \overset{\iota_\infty}{\hookrightarrow} M_2(\mathbb{R}). \\ \cup & & \cup \\ M_2(\mathbb{Z}) & \rightsquigarrow & \mathcal{O} \text{ order} \\ \cup & & \cup \\ SL_2(\mathbb{Z}) & & \mathcal{O}^1 := \{\gamma\in\mathcal{O} : \mathrm{nrd}(\gamma)=1\}. \hookrightarrow SL_2(\mathbb{R}) \end{array}$$

$E_\tau = \mathbb{C}/(\mathbb{Z}\tau+\mathbb{Z})$ $\qquad A_\tau = \mathbb{C}^2/\iota_\infty(\mathcal{O})\cdot\binom{\tau}{1}$

We will fix $F=\mathbb{Q}$, $D = \mathrm{disc}(B)\in\mathbb{Z}$. Let $\mathcal{O}\subset B$ be an order.

→ A subring, fin. gen. as a $\mathbb{Z}$-module, containing a $\mathbb{Q}$-basis of B.

equiv

→ The $\mathbb{Z}$-span of a $\mathbb{Q}$-basis of B that is closed under multiplication ($\mathbb{Z}$ is a PID).

Say $\mathcal{O}$ is maximal if it is so under inclusion.

Ex: $M_2(\mathbb{Z})\subseteq M_2(\mathbb{Q})$ maximal order.

Ex: If $a,b\in\mathbb{Z}\setminus\{0\}$, then $\mathcal{O} = \mathbb{Z}+\mathbb{Z}i+\mathbb{Z}j+\mathbb{Z}ij$ is an order.

MEx: $\mathcal{O} = \mathbb{Z}+\mathbb{Z}i+\mathbb{Z}j+\mathbb{Z}\left(\frac{1+i+j+ij}{2}\right)$ $\quad k^2-k-1=0.$ $\quad$ maximal order in $\left(\frac{-1,3}{\mathbb{Q}}\right)$.

$\quad$ $\underset{\text{"}k\text{"}}{}$

Let $B/\mathbb{Q}$ be indefinite. $\iota_\infty : B \hookrightarrow B\otimes_{\mathbb{Q}}\mathbb{R} \simeq M_2(\mathbb{R})$.

$B^1 := \{\gamma\in B^\times : \mathrm{nrd}(\gamma)=1\} = \ker\mathrm{nrd} \leq B^\times$; $\quad \mathcal{O}^1 = \mathcal{O}\cap B^1$.

Then $B^1 \hookrightarrow SL_2(\mathbb{R}) \circlearrowright \mathfrak{h}$ by LFT's. $\mathcal{O}^1 \subset SL_2(\mathbb{R})$ is a discrete group, in fact a Fuchsian group (= discrete ...). $\Rightarrow$ act properly on $\mathfrak{h}$.

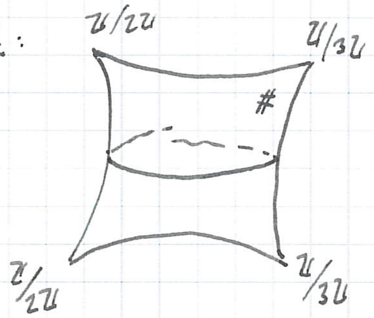
Let $\Gamma^1(\mathcal{O}) := \iota_\infty(\mathcal{O}^1)/\{\pm1\} \leq PSL_2(\mathbb{R})$.

$Y^1(\mathcal{O}) := \Gamma^1(\mathcal{O})\backslash\mathfrak{h}$ ← good complex 1-orbifold, compact ⟺ $B\not\simeq M_2(\mathbb{Q})$

$X^1(\mathcal{O}) := Y^1(\mathcal{O}) \cup$ cusps, compactification.

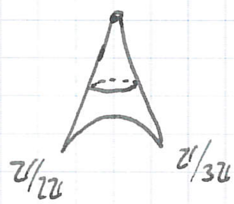
ALFRÉD RÉNYI INSTITUTE OF MATHEMATICS · HUNGARIAN ACADEMY OF SCIENCES
13 - 15 Reáltanoda u, H-1053 Budapest, Hungary | phone: +36 1 483 8300 | fax: +36 1 483 8333 | math@renyi.mta.hu | www.renyi.hu

Mex:



vs

Ex: $SL_2(\mathbb{Z})\backslash \mathfrak{h}$



To a point $\tau \in \mathfrak{h}$, associate $\Lambda_\tau := \underset{M_2(\mathbb{R})}{\underset{\cap}{\iota_\infty(\mathcal{O})}} \cdot \begin{pmatrix} \tau \\ 1 \end{pmatrix} \subseteq \mathbb{C}^2$

$A_\tau := \mathbb{C}^2 / \Lambda_\tau$.

Remark: $\iota_\infty = \iota_\tau : \mathcal{O} \hookrightarrow \mathrm{End}(A_\tau)$

$\Rightarrow$ A_τ is a complex torus of dimension 2 with endomorphisms by $\mathcal{O}$.

A principal polarization on $\mathcal{O}$ is an element $\mu \in \mathcal{O}$ s.t. $\mu^2 + D = 0$, $D := \mathrm{disc}(B)$.

$\rightarrow$ Every maximal order has one!

MEx: $\mu = 3i + ij = -1 + 2i - j + 2k$ $\quad$ (recall $k = \frac{1+i+j+ij}{2}$).

The involution $B \to B$; $\alpha \mapsto \alpha^* := \mu^{-1} \bar{\alpha} \mu$ is positive $(\mathrm{Tr}(\alpha\alpha^*) > 0 \ \forall \alpha \in B \setminus \{0\})$.

Ex: in $M_2(\mathbb{R})$, $\alpha^* = \bar{\alpha}^T$, $\mathrm{Tr}(\alpha^* \alpha) = 2(a^2+b^2+c^2+d^2)$ if $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

μ induces a principal polarization $\Leftrightarrow$ Riemann form on A_τ.

Main Theorem: The map $Y^1(\mathcal{O}) \longleftrightarrow \left\{ \begin{matrix} (A,\iota) \text{ principally polarized complex ab. surfaces} \\ \text{with QM by } (\mathcal{O},\mu) \end{matrix} \right\} / \cong$

$\Gamma\tau \longmapsto [(A_\tau, \iota_\tau)]$.

is a bijection. $\quad (\Gamma = \Gamma^1(\mathcal{O}))$

[QM by $(\mathcal{O},\mu)$ means ~~diagram~~

$$\begin{array}{ccc} B & \hookrightarrow & \mathrm{End}(A) \otimes \mathbb{Q} \\ \downarrow * \ \text{depends on } \mu & & \downarrow \dagger \\ B & \longleftrightarrow & \mathrm{End}(A) \otimes \mathbb{Q} \end{array}$$

commutes.]

Theorem (Shimura, Deligne):

There exists a nice curve $X^1_{\mathbb{Q}}$ defined over $\mathbb{Q}$ and a holomorphic map $\varphi : \mathfrak{h} \to X^1_{\mathbb{Q}}(\mathbb{C})$ that induces biholomorphism $\varphi : \Gamma^1 \backslash \mathfrak{h} \to X^1_{\mathbb{Q}}(\mathbb{C})$.

Mex (Baba-Granath)

$X^1_{\mathbb{Q}} : X^2 + 3Y^2 + Z^2 = 0 \subseteq \mathbb{P}^2$.

Thm (Ogg, Shimura): $X^1_{\mathbb{Q}}(\mathbb{R}) = \emptyset$.

§ Galois representations

A : abelian variety over a # field K. $G_K = \mathrm{Gal}(\bar{K}/K)$.

$A[n] \cong (\mathbb{Z}/n\mathbb{Z})^{2g}$, $g = \dim A$.

$$\rho_{A,n} : G_K \to \mathrm{Aut}(A[n]) \subseteq GL_{2g}(\mathbb{Z}/n\mathbb{Z}).$$

Weil pairing $\Rightarrow$ $\exists$ basis for $A[n]$ s.t.

$$\rho_{A,n}(\sigma)^t \, \Omega \, \rho_{A,n}(\sigma) = d_\sigma \Omega \quad , \quad \Omega = \left(\begin{array}{c|c} 0 & -I_g \\ \hline I_g & 0 \end{array}\right), \quad \text{where } \sigma(\zeta_n) = \zeta_n^{d_\sigma}.$$

$\Rightarrow$ Define $GSp_{2g}(R) := \{ M \in GL_{2g}(R) : M^t \Omega M = \lambda \cdot \Omega \text{ for some } \lambda \in R^\times \}$.

("group of symplectic similitudes").

Forcing $\lambda = 1$ we get $Sp_{2g}(R)$.

Choosing compatible bases we obtain

$$\rho_A : G_K \to GSp_{2g}(\hat{\mathbb{Z}}) = \varprojlim_n GSp_{2g}(\mathbb{Z}/n\mathbb{Z}).$$

For each $n \geq 1$, $\rho_{A,n} = \pi_n \circ \rho_A$, where $\pi_n : GSp_{2g}(\hat{\mathbb{Z}}) \to GSp_{2g}(\mathbb{Z}/n\mathbb{Z})$.

<u>Key point</u>: ρ_A is a continuous homomorphism (w.r.t. natural topologies in both grps).

<u>Rmk</u>: $GSp_2 = GL_2$.

<u>Thm</u> (Serre open image theorem)

If E/K is non-CM, then $\operatorname{im} \rho_E$ is <u>open</u> in $GL_2(\hat{\mathbb{Z}})$.

<u>Conjecture</u>:

$\exists N_d$ such that $\forall E/K$, $[K:\mathbb{Q}] = d$ and E non-CM,

$$\operatorname{im}(\rho_{E,\ell^\infty}) = GL_2(\mathbb{Z}_\ell) \quad \forall \ell > N_d. \qquad (\text{if } d=1,\ N_d = 37).$$

For $d=1$, one can prove that $\forall \ell > 37$,

$\operatorname{im} \rho_{E,\ell^\infty} \underset{\text{Mazur}}{\not\subset} \begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$, $\underset{\dots}{\not\subset} \begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix}$, but it could land in the normalizer of the non-split Cartan...

· <u>Generalization:</u>

Spse $\mathrm{End}(A_{\bar K}) = \mathbb{Z}$. <u>Serre</u>: $\dim A = 2, 6, \text{odd}$. Then $\mathrm{im}\, \rho_A$ is open in $GSp_{2g}(\hat{\mathbb{Z}})$.

<u>Absolute Frobenius:</u>

Let $p \in \mathbb{Z}$, pick a prime ideal in $\bar{\mathbb{Z}}$, say $\mathfrak{P}$, above p.

Let $\mathbb{F}_{\mathfrak{P}} := \bar{\mathbb{Z}}/\mathfrak{P}$. Then $\mathbb{F}_{\mathfrak{P}} \simeq \bar{\mathbb{F}}_p$, and $\mathrm{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_p) \simeq \hat{\mathbb{Z}}$.

Decomposition group:

$$D_{\mathfrak{P}} = \{ \sigma \in G_{\mathbb{Q}} : \sigma(\mathfrak{P}) = \mathfrak{P} \}.$$

Each element $\sigma \in D_{\mathfrak{P}}$ acts on $\mathbb{F}_{\mathfrak{P}} = \bar{\mathbb{Z}}/\mathfrak{P}$, $\sigma(x + \mathfrak{P}) = \sigma(x) + \mathfrak{P}$.

We obtain a surjective homomorphism; which gives rise to a s.e.s.:

$$1 \to I_{\mathfrak{P}} \to D_{\mathfrak{P}} \to \mathrm{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_p) \to 1.$$

An absolute Frobenius is any preimage $\mathrm{Frob}_{\mathfrak{p}} \in D_{\mathfrak{P}}$ of the Frobenius automorphism $x \mapsto x^p$.

$\mathrm{Frob}_{\mathfrak{p}}$ is only defined up to action of $I_{\mathfrak{P}} = \{ \sigma \in G_{\mathbb{Q}} : \sigma(x) \equiv x \bmod \mathfrak{P} \ \forall x \in \bar{\mathbb{Z}} \}$.

For any finite extension $K/\mathbb{Q}$, $\mathrm{Frob}_{\mathfrak{P}}|_K = \mathrm{Frob}_{(\mathfrak{P} \cap K)}$.

<u>Thm</u>: If $K/\mathbb{Q}$ is a finite extension in which p is unramified, then the conjugacy class of $\mathrm{Frob}_{\mathfrak{p}}|_K$ is uniquely determined.

Let $\mathfrak{P} \subseteq \mathcal{O}_K$ be a prime of good reduction for A/K.

$\mathfrak{P} \nmid n \Rightarrow \mathfrak{P}$ is unramified in $K(A[n])$.

$\rho_{A,n}(\mathrm{Frob}_{\mathfrak{P}}) = \pi_{A_{\mathfrak{P}}}|_{A[n]} \in GSp_{2g}(\mathbb{Z}/n\mathbb{Z})$

induced by $x \mapsto x^{\# \mathbb{F}_{\mathfrak{P}}}$, $\mathbb{F}_{\mathfrak{P}} = \mathcal{O}_K/\mathfrak{P}$.

& $\mathrm{charpoly}(\rho_{A,n}(\mathrm{Frob}_{\mathfrak{P}})) = \mathrm{charpoly}(\pi_{A_{\mathfrak{P}}}) \bmod n$.

§ Zeta functions

X : smooth projective curve over $\mathbb{F}_q$.

$$Z_X(T) = \exp\left(\sum_{n\geq 1} \#X(\mathbb{F}_q)\frac{T^n}{n}\right) = \frac{L(T)}{(1-T)(1-qT)}.$$

$L(T) \in \mathbb{Z}[T]$ of degree $2g$, roots α have $|\alpha| = q^{-1/2}$,

and so $L(T) = q^g T^{2g} + a_1 q^{g-1} T^{2g-1} + \dots + a_g T^g + a_{g-1}T^{g-1} + \dots + a_1 T + 1$.

(eg $a_1 = -\mathrm{tr}\, \pi_{\mathrm{Jac}(X)}$).

π_X is the Frobenius endomorphism of $\mathrm{Jac}(X)$; charpoly $(\pi_X) = T^{2g} L(T^{-1})$.

<u>Key Fact</u>: $Z_X(T)$ is determined by $\#X(\mathbb{F}_{q^n})$ $1 \leq n \leq g$.

If X is a smooth projective curve over # field, then

$$L(X,s) = \prod_{\mathfrak{p}} L_{\mathfrak{p}}(N(\mathfrak{p})^{-s})^{-1}.$$

—

Let now A/K be a QM abelian surface, with QM by $\mathcal{O}$. Let $\mathfrak{p}$ be a prime of K good for A.

Then $\mathcal{O} \subseteq \mathrm{End}(A_{\mathfrak{p}})$, and $\pi \in \mathrm{End}(A_{\mathfrak{p}})$.

$\Rightarrow$ $\mathrm{End}^0(A_{\mathfrak{p}})$ contains both $\mathcal{O}$ and the splitting field of charpoly (π).

By Albert's classification,

$$\mathrm{End}^0(A_{\mathfrak{p}}) \otimes_{\mathbb{Q}} \mathbb{R} \simeq \begin{cases} M_2(\mathbb{C}) & \text{ordinary} \\ M_2(\mathbb{H}) & \text{supersingular} \end{cases}$$

$\Rightarrow A_{\mathfrak{p}} \sim E^2$ for some $E/\mathbb{F}_{\mathfrak{p}}$.

Therefore, $L_{A_{\mathfrak{p}}}(T) = L_E(T)^2$.

Sometimes, QM abelian surfaces are called "fake elliptic curve", ~~but~~ but note that E depends on $\mathfrak{p}$!

Let's go back to $E/\mathbb{Q}$.

ker $\rho_{E,n} = \{\sigma \in G_{\mathbb{Q}} : \sigma|_{\mathbb{Q}(E[n])} = 1\}$

Im $\rho_{E,n} = \mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q}) \subseteq GL_2(\mathbb{Z}/n\mathbb{Z})$

Typically, im $\rho_{E,n} = GL_2(\mathbb{Z}/n\mathbb{Z})$, but <u>exceptions</u>

(1) E has extra level-~~n~~ structure, e.g. a rational point of order n, then im $\rho_{E,n} \subseteq \{\begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix} \leq GL_2(\mathbb{Z}/n\mathbb{Z})\}$

(note that $\{\begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix}\}$ has the same property...).

(2) E has CM ($\mathrm{End}(E) = \mathcal{O}$ order in imaginary quadratic).

Then $\mathrm{Gal}(K(E[n])/K)$ is abelian! But $GL_2(\mathbb{Z}/n\mathbb{Z})$ is not, so $\rho_{E,n}$ cannot be surjective.

Let E/K be an elliptic curve with CM by $\mathcal{O}$.

$E[n]$ is a free $\mathbb{Z}/n\mathbb{Z}$-module of rank 2.

<u>Claim</u>: $E[n]$ is a free $\mathcal{O}/n\mathcal{O}$-module of rank 1.

<u>Pf</u>: Fix $\mathbb{C}/\Lambda \cong E(\mathbb{C})$ (fix an embedding of $K \hookrightarrow \mathbb{C}$).

Then
$$E[n] \cong \tfrac{1}{n}\Lambda/\Lambda \quad \text{as } \mathcal{O}/n\mathcal{O}\text{-modules.}$$

CM by $\mathcal{O} \Rightarrow \mathcal{O}\Lambda \subseteq \Lambda$, and $\mathbb{C}/\Lambda$ is an $\mathcal{O}$-module.

For any prime ideal $\mathfrak{p} \subset \mathcal{O}$ s.t. $\mathfrak{p} \mid n$,

$$\tfrac{1}{n}\Lambda/\Lambda \otimes_{\mathcal{O}} \mathcal{O}/\mathfrak{p} \cong \tfrac{1}{n}\Lambda/\mathfrak{p}\tfrac{1}{n}\Lambda$$

Since $\mathcal{O}/n\mathcal{O} \cong \prod_{\mathfrak{p}|n} \mathcal{O}/\mathfrak{p}^e$, $E[n] \cong \prod_{\mathfrak{p}|n} \tfrac{1}{n}\Lambda/\mathfrak{p}^e\tfrac{1}{n}\Lambda$.

Let I be the fractional ~~ideal~~ $\mathcal{O}$-ideal $\frac{1}{n}\Lambda$. Then $I/\mathfrak{p}^e I$ is a free $\mathcal{O}/\mathfrak{p}^e$-module of rank 1. $\hat{\mathcal{O}} := \varprojlim \mathcal{O}/n\mathcal{O}$ ■

<u>Corollary</u>: $\mathrm{im}(\rho_E) \subseteq GL_1(\hat{\mathcal{O}}) = \hat{\mathcal{O}}^\times \subsetneq GL_2(\hat{\mathbb{Z}})$.

We obtain that

im $\rho_{E,p}$ depends on whether p is $\begin{cases} \text{split} & (\mathcal{O}/p)^\times \simeq (\mathbb{F}_p^\times)^2 \\ \text{inert} \; \cancel{\text{non split}} & (\mathcal{O}/p)^\times \simeq \mathbb{F}_{p^2}^\times \\ \text{ramified} & (\mathcal{O}/p)^\times \simeq \mathbb{F}_p^\times . \end{cases}$

Now, suppose that A/K is a QM abelian surface with QM by $\mathcal{O}$ ← order in a quaternion algebra.

Claim: $A[n]$ is a free $\mathcal{O}/n\mathcal{O}$-module of rank 1.

Pf Follow the CM case, now the lattice in $\mathbb{C}^2/\Lambda$, $\mathcal{O}n$ is a two-sided ideal... ∎

Now, im$(\rho_A) \subseteq GL_1(\hat{\mathcal{O}}) \simeq \hat{\mathcal{O}}^\times \subseteq GSp_4(\hat{\mathbb{Z}})$.

The mod p image im$(\rho_{A,p})$ depends on whether $\begin{cases} \text{unramified}: & (\mathcal{O}/p\mathcal{O})^\times \simeq GL_2(\mathbb{Z}/p\mathbb{Z}) \\ \text{ramified}: & \text{exercise.} \end{cases}$

Suppose that A/K is a QM abelian surface with a rational point of order n.

$A[n]$ is an $\mathcal{O}$-module, so ~~..~~ $A(K)[n]$ must contain $\mathcal{O}.P$ (a cyclic $\mathcal{O}$-module).

If n is coprime to disc$(\mathcal{O})$, then $\mathcal{O}.P \simeq (\mathbb{Z}/n\mathbb{Z})^2$.

ALFRÉD RÉNYI INSTITUTE OF MATHEMATICS · HUNGARIAN ACADEMY OF SCIENCES
13-15 Reáltanoda u, H-1053 Budapest, Hungary | phone: +36 1 483 8300 | fax: +36 1 483 8333 | math@renyi.mta.hu | www.renyi.hu

Goal: work explicitly with Shimura curves.

1. Fundamental domains.
2. Equations using power series expansions of modular forms.

Let $\Gamma \leq PSL_2(\mathbb{R})$ be a Fuchsian group s.t $Y(\Gamma) := \Gamma \backslash \mathfrak{h}$ has finite hyperbolic area.

A fundamental domain $\square \subseteq \mathfrak{h}$ for Γ is
wasylozenge

(i) $cl(\operatorname{int} \square) = \square$.

(ii) $\Gamma \square = \mathfrak{h}$,

(iii) $\operatorname{int} \square \cap \operatorname{int} \gamma\square = \emptyset \quad \forall \gamma \neq 1, \gamma \in \Gamma$, and

(iv) $\mu(bd(\square)) = 0$.

Let $z_0 \in \mathfrak{h}$ be s.t $Stab_\Gamma(z_0) = \{1\}$. The Dirichlet domain for Γ at z_0 is:

$$\square := \square(\Gamma; z_0) := \{ z \in \mathfrak{h} : \underset{\text{hyperbolic distance}}{\rho}(z, z_0) \leq \rho(\gamma z, z_0) \ \forall \gamma \in \Gamma \}.$$

Then:

$$\square = \bigcap_{\gamma \in \Gamma} H(\gamma, z_0), \quad \text{where} \quad H(\gamma, z_0) = \{ z \in \mathfrak{h} : \rho(z, z_0) \leq \overset{\rho(z, \gamma^{-1} z_0)}{\overset{\parallel}{\rho(\gamma z, z_0)}} \}.$$

Ex: $\square(PSL_2(\mathbb{Z}); 2i)$  (usual one).

Thm: $\square(\Gamma, z_0)$ is a connected, convex, locally finite ($\forall K \subseteq \mathfrak{h}$ compact, $\gamma K \cap \square \neq \emptyset$ for only finitely many $\gamma \in \Gamma$) fundamental domain for Γ, with geodesic boundary.

Let $\varphi : \mathfrak{h} \to \mathbb{D} = \{ z \in \mathbb{C} : |z| < 1 \}$.

$$z \longmapsto \frac{z - z_0}{z - \bar{z}_0} =: w$$

For $\gamma \in \Gamma$, let $I(\gamma) = \{ w \in \mathbb{C} : |cw + d| = 1 \}$ (isometric circle), if $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

The action $\Gamma \leq PSL_2(\mathbb{R})$ on $\mathfrak{h}$ becomes an action $\leq PSU(1,1) \subseteq GL_2(\mathbb{C})$ on the unit disk.

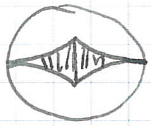
Then
$$\rho(w, 0) \left\{ \begin{matrix} < \\ = \\ > \end{matrix} \right\} \rho(\gamma w, 0) \iff w \in \left\{ \begin{matrix} ext(I(\gamma)) \\ I(\gamma) \\ \operatorname{int}(I(\gamma)) \end{matrix} \right.$$

ALFRÉD RÉNYI INSTITUTE OF MATHEMATICS · HUNGARIAN ACADEMY OF SCIENCES
13 – 15 Reáltanoda u, H-1053 Budapest, Hungary | phone: +36 1 483 8300 | fax: +36 1 483 8333 | math@renyi.mta.hu | www.renyi.hu

So $\square(\Gamma; 0) = \bigcap_{\gamma\in\Gamma\setminus\{1\}} \mathrm{cl}\,\mathrm{Ext}\, I(\gamma)$.

If $\Gamma_0 := \mathrm{Stab}_\Gamma(z_0) \neq \{1\}$, then $\square = \bigcup_{\gamma_0\in\Gamma_0} \gamma_0 \square'$, where $\square' = \square \cap$  $2\pi/\#\Gamma_0$.

and $\square'$ is a fundamental domain for Γ.

Ex: $\square(PSL_2(\mathbb{Z}), i) =$  $\longleftrightarrow$ 

A side of $\square$ is a geodesic segment $\square\cap\gamma\square$, $\gamma\in\Gamma\setminus\{1\}$, except with the convention if $L=\square\cap\gamma\square$, $\gamma^2=1$, then γ fixes the midpoint of L, and we double it (consider it as two sides).

Thm: Γ is generated by the side pairing elements $\{\gamma\in\Gamma : \square\cap\gamma\square\neq\emptyset\}$.
Relations can be read off from vertices.

MEx: $\Gamma := \iota_\infty(\mathcal{O}^1)/\{\pm1\} \le PSL_2(\mathbb{R})$. $\varphi(z) = w = \frac{z-i}{z+i}$.

$\gamma = t+xi+yj+zij \in \mathcal{O}^1$

$\varphi_*(\gamma) = \begin{pmatrix} t-ix & \sqrt{3}(y-iz) \\ \sqrt{3}(y+iz) & t+ix \end{pmatrix} \in SU(1,1)$. $\quad |w+\frac{d}{c}| = \frac{1}{|c|}$ $\Updownarrow$

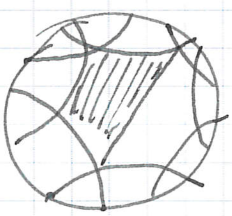
We compute the center & radius of $I(\gamma) = \{w : |cw+d| = 1\}$:

i.e. center $= -\frac{d}{c} = \frac{-(t+ix)}{\sqrt{3}(y+iz)}$ radius $= \frac{1}{\sqrt{3(y^2+z^2)}}$.

unless $y^2+z^2=0 \iff y=z=0 \iff \gamma=\pm1,\pm i \iff \gamma\in\langle i\rangle$.

$y^2+z^2 = 1/4$ doesn't arise b/c $\mathrm{nrd}(\gamma): t^2+x^2-3(y^2+z^2)=1$.

$y^2+z^2 = \frac{1}{2} \Rightarrow y,z = \pm\frac{1}{2}$, $t^2+x^2 = 5/2 \Rightarrow \gamma = \pm\frac{3}{2}\pm\frac{1}{2}i\pm\frac{1}{2}j\pm\frac{1}{2}ij$ or
$\pm\frac{1}{2}\pm\frac{3}{2}i\pm\frac{1}{2}j\pm\frac{1}{2}ij$.



$\rightsquigarrow \Gamma = \langle \gamma_1,\gamma_2,\gamma_3 \mid \gamma_1^2=\gamma_2^3=\gamma_3^3=(\gamma_3\gamma_2\gamma_1)^2=1\rangle$

$= \langle \gamma_1,\gamma_2,\gamma_3,\gamma_4 \mid \gamma_1^2=\gamma_2^3=\gamma_3^3=\gamma_4^2=\gamma_4\gamma_3\gamma_2\gamma_1=1\rangle$.

Suppose that $Y(\Gamma) = X(\Gamma)$ is compact, so no cusps.

Def: A modular form f of weight $k \in 2\mathbb{Z}_{\geq 0}$ for Γ is a holomorphic map $f : \mathfrak{h} \to \mathbb{C}$ s.t.

- $f(\gamma z) = (cz+d)^k f(z) \quad \forall\, \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma \leq PSL_2(\mathbb{R})$.

Write
$$f(z) = (1-w)^k \sum_{n=0}^{\infty} b_n w^n \in M_k(\Gamma) \text{: modular form of weight } k \text{ and level } \Gamma.$$

Ex: $f \in S_2(\Gamma_0(11)) \qquad f = q \prod_{n=1}^{\infty} (1-q^n)^2 (1-q^{11n})^2$.

At $z_0 = \frac{-9+\sqrt{-7}}{22}$, it has expansion
$$f(z) = c_0 (1-w)^2 \left(1 - \Theta w + \frac{5}{2!}(\Theta w)^2 - \frac{123}{3!}(\Theta w)^3 - \dots\right)$$

$\Theta = \frac{4+2\sqrt{-7}}{11} \pi \Omega^2$, $\quad \Omega = 0{,}500441\ldots \in$ Chowla - Selberg period.

How to do this in general ??
$$f(z) \approx f_N(z) = (1-w)^k \sum_{n=0}^{N} b_n w^n \quad \text{valid for } |w| \leq \rho \text{ to precision } \varepsilon > 0.$$

$z' \in \mathfrak{h} \qquad z \in \mathfrak{h}$

For $w \notin \square$, $|w| \leq \rho$, $\exists\, \gamma \in \Gamma$ s.t. $w' = \gamma w \in \square \qquad \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

So
$$f_N(z') \approx f(z') = (cz+d)^k f(z) \approx (cz+d)^k f_N(z).$$

$$\therefore \boxed{(1-w')^k \sum_{n=0}^{N} b_n (w')^n \approx (cz+d)^k (1-w)^k \sum_{n=0}^{N} b_n w^n}.$$

This gives linear relations for b_n's !.

When $\Gamma \leq \Delta$ with Δ a triangle group, we can certify output as rigorous.

<u>Thm</u> (Valence formula) (Shimura):

$$\dim_{\mathbb{C}} M_k(\Gamma) = \begin{cases} 1 & k=0 \\ g & k=2 \\ (k-1)(g-1) + \sum_{i=1}^{r} \left\lfloor \frac{k}{2}\left(1-\frac{1}{e_i}\right)\right\rfloor & k \geq 4 \end{cases}.$$

where Γ has signature $(g; e_1, \ldots, e_r)$ (no cusps) $\begin{cases} g = \text{genus} \\ e_i = \text{orders of stabilizers} \end{cases}$

<u>MEx</u>: $\mathrm{Sig}(\Gamma) = (0; 2,2,3,3)$

$$\dim = \begin{cases} 1 & k=0 \\ 0 & k=2 \\ 1-k + 2\left\lfloor \frac{k}{4}\right\rfloor + 2\left\lfloor \frac{k}{3}\right\rfloor & k \geq 4 \end{cases}$$

k	0	2	4	6	8	10	12	...	24
dim	1	0	1	1	1	1	3	...	5
span	1	-	f_4	g_6	f_4^2	$f_4 g_6$	f_4^3, g_6^2, h_{12}		$f_4^6, f_4^3 g_6^2, f_4^3 h_{12}, g_6^4, g_6^2 h_{12}, h_{12}^2$

$$\Rightarrow M(\Gamma) = \bigoplus_{k \in 2\mathbb{Z}_{\geq 0}} M_k(\Gamma) \simeq \frac{\mathbb{C}[x_4, x_6, x_{12}]}{(x_4^6 + 3x_6^4 + x_{12}^2)}$$

$$X(\Gamma) = \mathrm{Proj}\, M(\Gamma) \subseteq \mathbb{P}(4,6,12) \hookrightarrow \mathbb{P}^2$$

$$(x:y:z) \longmapsto (x^3 : y^2 : z).$$