INTRODUCTION TO SHIMURA CURVES, I

Pilar Bayer

Universitat de Barcelona

•

Mathematisches Institut, Georg-August-Universität, Göttingen

July, 2004

Overview of results on Shimura curves

- general theory and L-functions: Shimura 1959-1970
- integral models: Ihara 1969, 1971; Morita 1981; Carayol 1986; Jordan-Livné 1986; Buzzard 1997; Sasaki 2001
- complex uniformization: Ihara 1974; Michon 1980; Alsina 1999, Johansson 2001
- p-adic uniformization: Cerednik 1976; Drinfeld 1976; Zink 1982; Boutot-Carayol 1991

- hyperelliptic and bielliptic cases: Ishii 1975; Michon 1981; Ogg 1983, 1985; Rotger 2001

- equations: Kurihara 1979; Jordan-Livné 1981; Kurihara 1994

- diophantine properties: Jordan-Livné 1985, 1987, 1999; Ogg 1985; Kamienny 1990; Elkies 1998

Some applications of Shimura curves

- connections with modular curves and applications to FLT: Ribet 1980, 1990; Diamond-Taylor 1994; Diamond 1997

- applications to the theory of error-correcting-codes: Tsfasman-Vladut-Zink 1982

- connections with p-adic L-functions and Birch and Swinnerton-Dyer conjecture: Bertolini-Darmon 1996, 1998

Introduction to Shimura curves

I: Fundamental domains and CM-points (M. Alsina, P. Bayer)

II: Uniformization of Shimura curves (A. Travesa, P. Bayer)

III: Abelian varieties with QM (J. Guàrdia, V. Rotger, P. Bayer)

[...] The last part of the paper is devoted to the theory of a certain type of automorphic functions of one variable known in the literature as functions belonging to indefinite ternary quadratic forms [H. Poincaré 1887], [R. Fricke u. F. Klein 1897]; they occur as moduli of abelian varieties of dimension 2 whose endomorphism rings are isomorphic to an order of an indefinite quaternion algebra.

G. Shimura [*On the theory of automorphic functions*,1959]

Envisageons une forme quadratique indéfinie F à coefficients entiers [...]. Considérons le groupe principal de F formé de toutes les substitutions à coefficients entiers qui n'altèrent pas cette forme. [...] au groupe principal de F correspondra un groupe fuchsien G, qui sera le groupe fuchsien principal de F.

H. Poincaré [*Les fonctions fuchsiennes et l'arithmétique*, 1887]

Hyperbolic plane

$$\mathcal{H} = \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$$

$$d(z_1, z_2) = \left| \operatorname{arc\,cosh} \left(1 + \frac{|z_1 - z_2|^2}{2\,\mathrm{Im}(z_1)\,\mathrm{Im}(z_2)} \right) \right|$$

Hyperbolic lines: semilines orthogonal to $\mathbb{R}$,
semicercles centered on real points

$$\mathbf{PSL}(2, \mathbb{R}) = \mathbf{GL}^{+}(2, \mathbb{R})/\mathbb{R}^{*}1_2 = \mathbf{SL}(2, \mathbb{R})/\{\pm 1_2\}$$

$$\alpha = \begin{bmatrix} a & b \\ c & d \end{bmatrix}, \quad \alpha(z) = \frac{az + b}{cz + d}$$ homographic transformations

Fixed points of homographic transformations

$$\alpha = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathbf{SL}(2,\mathbb{R}),\ \alpha \neq \pm 1_2,\ \alpha(z) = z \Leftrightarrow z = \frac{a-d \pm \sqrt{(a+d)^2-4}}{2c}$$

hyperbolic: $|\mathrm{tr}(\alpha)| > 2$, $\{z_1, z_2\}$, $z_1, z_2 \in \mathbb{R} \cup \{\infty\}$, $\begin{bmatrix} \lambda_1 & \\ & \lambda_2 \end{bmatrix}$

elliptic: $|\mathrm{tr}(\alpha)| < 2$, $\{z, \overline{z}\}$, $z \in \mathcal{H}$, $\begin{bmatrix} e^{i\theta} & \\ & e^{-i\theta} \end{bmatrix}$, $0 < \theta < 2\pi$

parabolic: $\mathrm{tr}(\alpha) = \pm 2$, $\{z\}$, $z \in \mathbb{R} \cup \{\infty\}$, $\begin{bmatrix} \pm 1 & 1 \\ 0 & \pm 1 \end{bmatrix}$

Fuchsian groups of the first kind

$\Gamma \leq \mathbf{SL}(2,\mathbb{R})$ discrete subgroup, $\overline{\Gamma} \leq \mathbf{PSL}(2,\mathbb{R})$, $\mathcal{H}^* = \mathcal{H} \cup \mathcal{P}_\Gamma$

$\pi : \mathcal{H}^* \to \overline{\Gamma}\backslash\mathcal{H}^*$, $j_{\overline{\Gamma}} : \overline{\Gamma}\backslash\mathcal{H}^* \sim X(\overline{\Gamma})(\mathbb{C})$ compact Riemann surface

$$z \in \mathcal{H}, \quad \#\overline{\Gamma}_z = \begin{cases} \infty \\ e > 1 \\ 1 \end{cases}, \quad \tfrac{1}{2\pi} v(\overline{\Gamma}\backslash\mathcal{H}^*) = 2g - 2 + \sum_{w \in X(\overline{\Gamma})} \left(1 - \frac{1}{e_w}\right)$$

$[\overline{\Gamma} : \overline{\Gamma}'] = n$, $\varphi :\ X(\overline{\Gamma}') \to X(\overline{\Gamma})$, $e_{w,\varphi} = [\overline{\Gamma}_{\varphi(w)} : \overline{\Gamma}'_w]$

$$2g' - 2 = n(2g-2) + \sum_{w \in X(\overline{\Gamma}')} (e_{w,\varphi} - 1) \quad \text{Hurwitz formula}$$

Fundamental domains for $\overline{\Gamma}$

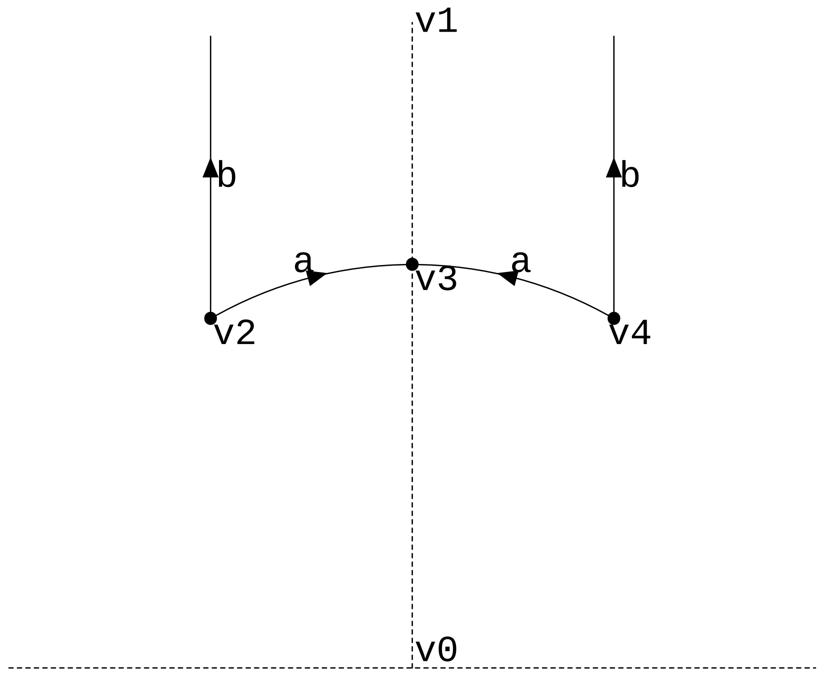
(i) $\mathcal{D} = \mathcal{D}(\overline{\Gamma}) \subseteq \mathcal{H}$ connected, $\quad \mathcal{H} = \bigcup_{\gamma \in \Gamma} \gamma(\mathcal{D})$,

(ii) $\mathcal{D} = \overline{U}$, $\quad U$ open set, $\quad U = \mathrm{int}(\mathcal{D})$,

(iii) $\gamma(U) \cap U = \emptyset$, $\quad$ for any $\gamma \in \Gamma$, $\gamma \neq \pm 1_2$.

- Every Fuchsian group of the first kind possesses a fundamental polygon

- Fundamental half domain: it contains all the vertices of a fundamental domain exactly once



$\Gamma = \mathbf{SL}(2, \mathbb{Z})$, modular group

Automorphic forms

$$\alpha = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathbf{GL}^+(2,\mathbb{R}), \quad j(\alpha,z) = cz + d$$

$$f:\ \mathcal{H} \to \mathbb{P}^1, \quad k \in \mathbb{Z}, \quad (f|_k\alpha)(z) := \det(\alpha)^{k/2} j(\alpha,z)^{-k} f(\alpha z), \quad z \in \mathcal{H}$$

$\mathcal{A}_k(\Gamma)$:

$f(z)$ meromorphic on $\mathcal{H}$ and at all cusps; $\quad f|_k\gamma = f,$ for all $\gamma \in \Gamma$

$$\mathcal{A}_0(\Gamma) \simeq \mathbb{C}(X(\overline{\Gamma}))$$

$$\mathcal{A}_{2m}(\Gamma) \simeq D^m(X(\overline{\Gamma})), \quad f \mapsto \omega_f, \quad f(z)(dz)^m = \omega_f \circ \pi$$

$$f \in \mathcal{A}_0(\Gamma) \Rightarrow D(f,z) \in \mathcal{A}_2(\Gamma)$$

Schwarzian derivative $D_s(f,z) := \dfrac{2D(f,z)D^3(f,z) - 3D^2(f,z)^2}{D(f,z)^2}$

Automorphic derivative $D_a(f,z) := \dfrac{D_s(f,z)}{D(f,z)^2}$

$$D_a(\frac{az+b}{cz+d}, z) = 0, \quad \text{for all } \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathbf{GL}(2,\mathbb{C})$$

$$D_a(g \circ f, z) = D_a(g, f(z)) + \frac{D_a(f,z)}{D(g,f(z))^2}$$

$$f^{-1}(w) = z, \quad D_s(f^{-1}(w)) = -D_a(f,z)$$

$f(z) \in \mathcal{A}_0(\Gamma) \Rightarrow D_a(f,z) \in \mathcal{A}_0(\Gamma)$ Schwarz, 1873

Theorem. *Let $\overline{\Gamma}$ be a Fuchsian group of the first kind such that $X(\overline{\Gamma})$ is a curve of genus 0. Assume that we are aware of a fundamental half domain for the action of $\overline{\Gamma}$ in $\mathcal{H}^*$. Suppose that t is a generator of the field of $\overline{\Gamma}$-automorphic functions such that its values at the vertices of the fundamental half domain belong to $\mathbf{P}^1(\mathbb{R})$. Then, there exists a rational function $R(t)$ such that*

$$Da(t, z) + R(t) = 0.$$

If $\alpha_i \pi$ are the internal angles at the vertices of the fundamental half domain, then

$$R(t) = \sum \frac{1 - \alpha_i^2}{(t - a_i)^2} + \sum \frac{B_i}{t - a_i},$$

where B_i are constants and the summation extends over all the vertices of the fundamental half domain where the function t takes finite values a_i.

If the values of t at all the vertices are finite, then

(a) $\sum B_i = 0$,

(b) $\sum a_i B_i + \sum(1 - \alpha_i^2) = 0$,

(c) $\sum a_i^2 B_i + \sum a_i(1 - \alpha_i^2) = 0$.

If ∞ is the value of t at a vertex with internal angle $\alpha\pi$, then

(a) $\sum B_i = 0$,

(b) $\sum a_i B_i + \sum(1 - \alpha_i^2) - (1 - \alpha^2) = 0$. □

In general, the above relations between the constants B_i, the angles α_i, and the values a_i do not suffice to determine all the constants.

Fuchs, Schwarz, Dedekind, Klein, Poincaré

Example: Valence function

$$[v,z] = \frac{-4}{\sqrt{\frac{dv}{dz}}}\frac{d^2}{dv^2}\sqrt{\frac{dv}{dz}} = -Da(v,z) = Ds(z,v)$$

$$v(i) = 1, \quad v(e^{\frac{2\pi i}{3}}) = 0, \quad v(\infty) = \infty$$

$$\frac{1}{(1-v)^{1/2}}\frac{dv}{dz}, \quad \frac{1}{v^{2/3}}\frac{dv}{dz}, \quad \frac{1}{v}\frac{dv}{dz}$$

Fuchs theory: $F(v) = \frac{3}{4(1-v)^2} + \frac{8}{9v^2} + \frac{23}{36(1-v)} + \frac{23}{36v} = \frac{36v^2-41v+32}{36v^2(1-v)^2}$

$$[v,z] = F(v), \qquad \frac{d^2\eta}{dv^2} = -\frac{1}{4}F(v)\eta, \; z(v) = \frac{\eta_1(v)}{\eta_2(v)}$$

Dedekind, 1877

$$j(q) = 1728\, v(q), \qquad q(z) = \exp(2\pi i z)$$

$j = 1728\, \frac{g_2^3}{\Delta}$

$$g_2(\tau) = 60 \sum_{\substack{m,n\in\mathbb{Z} \\ (m,n)\neq(0,0)}} \frac{1}{(m\tau+n)^4}, \qquad g_3(\tau) = 140 \sum_{\substack{m,n\in\mathbb{Z} \\ (m,n)\neq(0,0)}} \frac{1}{(m\tau+n)^6}$$

$\Delta(\tau) = g_2(\tau)^3 - 27 g_3(\tau)^2 \neq 0$

- $\mathbb{C}/\langle 1, \tau\rangle \xrightarrow{\sim} E_\tau(\mathbb{C}), \qquad {\wp'}^2(z) = 4\wp^3(z) - g_2(\tau)\wp(z) - g_3(\tau)$

$$E_\tau \simeq E_{\tau'} \Longleftrightarrow j(\tau) = j(\tau')$$

$$j(q) = \frac{1}{q} + 744 + 196884q + 21493760q^2$$

$$+864299970q^3 + 20245856256q^4$$

$$+333202640600q^5 + 4252023300096q^6$$

$$+44656994071935q^7 + O(q^8)$$

$$q(z) = e^{2\pi iz}, \qquad q(z+1) = q(z)$$

$$j(q(z+1)) = j(q(z)), \quad j(q(-1/z)) = j(q(z)), \quad j(q(-\overline{z})) = \overline{j(q(z))}$$

$$j : \mathbf{PSL}(2,\mathbb{Z})\backslash\mathcal{H}^* \to \mathbb{P}^1(\mathbb{C})$$

Quaternion algebras

$$H = \left(\frac{a,b}{\mathbb{Q}}\right) = \langle 1, i, j, k \rangle, \qquad i^2 = a, \quad j^2 = b, \quad ij = -ji = k$$

$$\alpha = x+yi+zj+tk \mapsto \overline{\alpha} = x-yi-zj-tk, \qquad \mathrm{Tr}(\alpha) = \alpha+\overline{\alpha}, \quad \mathrm{Nr}(\alpha) = \alpha\overline{\alpha}$$

$$H \otimes \mathbb{Q}_v = \begin{cases} \mathbf{M}(2, \mathbb{Q}_v) & \text{unramified at } v, \\ \\ \mathbb{H}_v \text{ skew field} & \text{ramified at } v \end{cases} \qquad D_H = \prod_{v_p \, \text{ram}} p$$

H indefinite, $a > 0$, $\quad \Phi : \; H \hookrightarrow \mathbf{M}(2, \mathbb{R})$

$$\Phi(x + yi + zj + tk) = \begin{bmatrix} x + y\sqrt{a} & z + t\sqrt{a} \\ b(z - t\sqrt{a}) & x - y\sqrt{a} \end{bmatrix}$$

Examples $\quad H \otimes_{\mathbb{Q}} \mathbb{R} \simeq \mathbf{M}(2,\mathbb{R})$ indefinite

- $D_H = 1, \quad H \simeq \mathbf{M}(2,\mathbb{Q}) \simeq \left(\dfrac{1,-1}{\mathbb{Q}}\right)$

- $D_H = pq$

type A: $H_A(p) = \left(\dfrac{p,-1}{\mathbb{Q}}\right)$, $D_H = 2p$, $p \equiv 3 \pmod 4$; $\quad D_H = 6, 14, \ldots$

type B: $H_B(p,q) = \left(\dfrac{p,q}{\mathbb{Q}}\right)$, $D_H = pq$, $q \equiv 1 \pmod 4$ and $\left(\dfrac{p}{q}\right) = -1$;
$D_H = 10, 15, \ldots$

Orders in quaternion algebras

$\mathcal{O} \subseteq H$ subring, $\mathbb{Z}$-module of rank 4;

$\mathcal{O}(D,N)$ Eichler order of level $N \geq 1$, $\gcd(D,N) = 1$, $\square \nmid N$

$$\mathcal{O}_0(1,N) = \left\{ \begin{bmatrix} a & b \\ cN & d \end{bmatrix} : a,b,c,d \in \mathbf{M}(2,\mathbb{Z}) \right\}$$

$$\mathcal{O}_A(2p,N) = \mathbb{Z}\left[1, i, Nj, \frac{1+i+j+k}{2}\right], \; N | \tfrac{p-1}{2}$$

$$\mathcal{O}_B(pq,N) = \mathbb{Z}\left[1, Ni, \frac{1+j}{2}, \frac{i+k}{2}\right], \; N | \frac{q-1}{4}, \; \gcd(N,p) = 1$$

Fuchsian groups of quaternion units

$H \otimes \mathbb{R} \simeq \mathbf{M}(2, \mathbb{R})$, $\mathcal{O}(D, N)$ Eichler order

$\Gamma(D, N) := \Phi(\{x \in \mathcal{O} : \mathrm{Nr}(x) = 1\}) \leq \mathbf{SL}(2, \mathbb{R})$ arithmetic group

$\Gamma(1, 1) = \mathbf{SL}(2, \mathbb{Z})$, $\Gamma(1, N) = \Gamma_0(N)$

$X(1, N)/\mathbb{Q} = X_0(N)/\mathbb{Q}$ modular curve; $X(D, N)/\mathbb{Q}$ Shimura curve

$$j_{D,N} : \overline{\Gamma}(D, N)\backslash\mathcal{H}^* \sim X(D, N)(\mathbb{C})$$

$j_{1,1}(z) = j(z)$; $j_{1,N}(z) = (j(z), j(Nz))$

Fuchsian groups $\overline{\Gamma}(D, N)$

- $\mathcal{O}_A(2p, N)$

  $\Gamma(2p, N) =$
  $$\left\{\gamma = \tfrac{1}{2}\begin{bmatrix} \alpha & \beta \\ -\beta' & \alpha' \end{bmatrix} : \alpha, \beta \in \mathbb{Z}[\sqrt{p}],\ \alpha \equiv \beta \equiv \alpha\sqrt{p} \pmod 2, \right.$$
  $$\left. N|(\mathrm{tr}(\beta) - \tfrac{\beta-\beta'}{\sqrt{p}}),\ \det(\gamma) = 1, \right\}$$

- $\mathcal{O}_B(pq, N)$

  $$\Gamma(pq, N) = \left\{\gamma = \frac{1}{2}\begin{bmatrix} \alpha & \beta \\ q\beta' & \alpha' \end{bmatrix} : \alpha, \beta \in \mathbb{Z}[\sqrt{p}], \alpha \equiv \beta \pmod 4, \right.$$
  $$\left. N \mid \tfrac{\alpha-\alpha'-\beta+\beta'}{2\sqrt{p}}, \det(\gamma) = 1 \right\}$$

Fundamental domains: $D > 1$

$\Gamma(D,N)$, $\quad \mathcal{O}(D,N) \subseteq H = \left(\frac{a,b}{\mathbb{Q}}\right)$, $a > 0$, $\quad \Phi : H \hookrightarrow \mathbf{M}(2, \mathbb{Q}(\sqrt{a}))$

Pell equation: ε fundamental unit in $\mathbb{Q}(\sqrt{a})$

$\xi := \varepsilon$ if $n(\varepsilon) = 1$, $\xi := \varepsilon^2$ if $n(\varepsilon) = -1$, $h := \begin{bmatrix} \xi & \\ & \xi' \end{bmatrix}$, $\quad h^s(z) = \xi^{2s} z$

1. There exists $s \geq 1$ such that $h^s \in \Gamma(D,N)$, $\overline{\Gamma}(D,N)_\infty = \langle h^s \rangle$.

2. The hyperbolic strip $\left\{ z \in \mathcal{H} : r \leq |z| \leq \xi^{2s} r \right\}$ yields a fundamental domain for $\overline{\Gamma}(D,N)_\infty$, where $r \in \mathbb{R}^+$.

A fundamental domain for $X(6,1)$

1. The hyperbolic hexagon $[v_1, v_2, v_3, v_4, v_5, v_6]$ yields a fundamental domain for $\overline{\Gamma}(6,1)$, where $v_1 = \dfrac{-\sqrt{3}+i}{2}$, ...

2. All the vertices v_i are elliptic and $\gamma_{v_1} = \begin{bmatrix} \sqrt{3} & 2 \\ -2 & -\sqrt{3} \end{bmatrix}$, ...

3. $V(6,1) = \dfrac{2\pi}{3}, \quad g(6,1) = 0.$

4. Elliptic cycles of order 2: $\{v_6\}$, $\{v_1, v_3, v_5\}$.

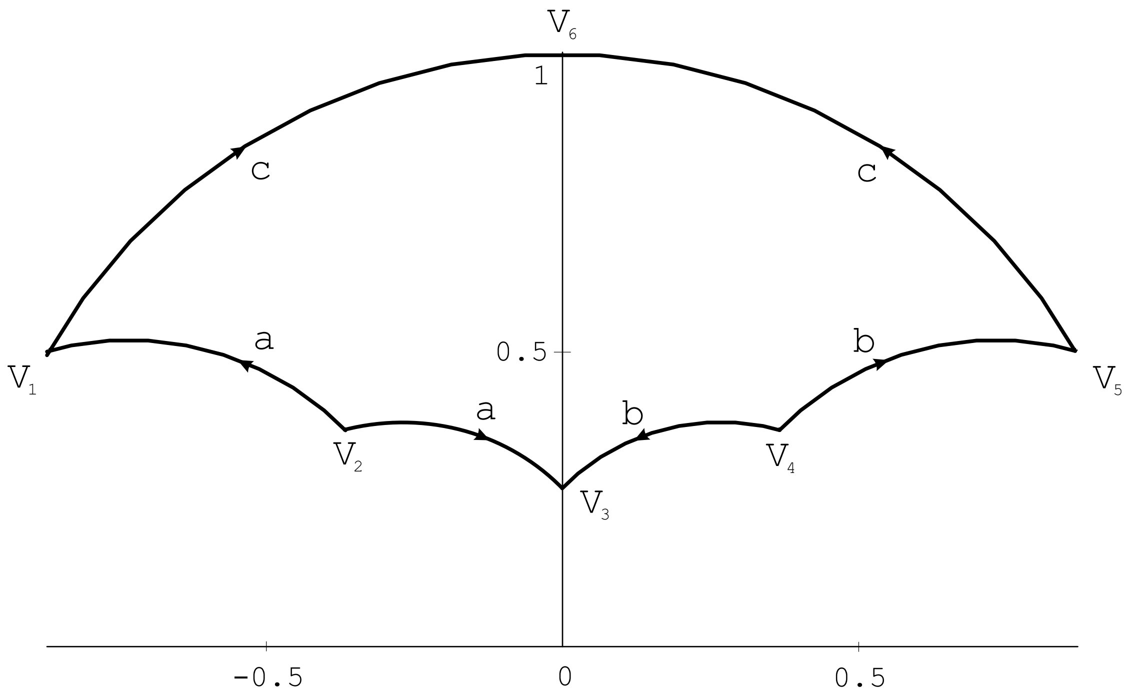
5. Elliptic cycles of order 3: $\{v_2\}$, $\{v_4\}$.

6. The principal homothety of $\Gamma(6,1)$ is $h = \begin{bmatrix} 2+\sqrt{3} & 0 \\ 0 & 2-\sqrt{3} \end{bmatrix}$.

7. The pairing is (v_2v_3, v_2v_1) by γ_{v_2}; (v_3v_4, v_5v_4) byγ_{v_4}; (v_5v_6, v_1v_6) by γ_{v_6}.

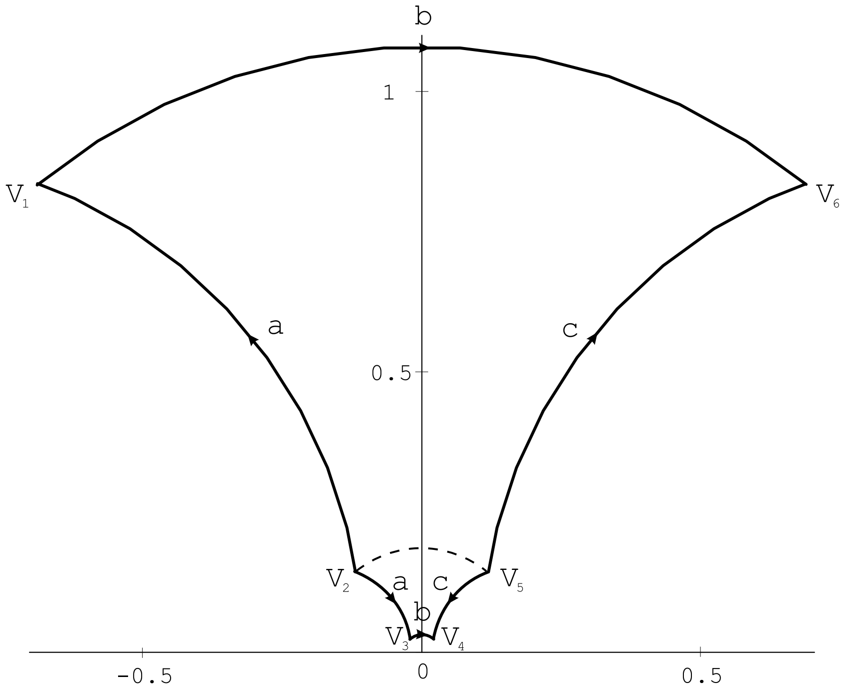
8. $\overline{\Gamma}(6,1) = \langle \gamma_{v_2}, \gamma_{v_4}, \gamma_{v_6} : \gamma_{v_2}^3 = \gamma_{v_4}^3 = \gamma_{v_6}^2 = (\gamma_{v_2}^{-1}\gamma_{v_6})\gamma_{v_4})^2 = 1\rangle$.

9. $\mathcal{D}(6,1)$ is invariant with respect to $w = \frac{1}{\sqrt{6}}\begin{bmatrix} 0 & -3+\sqrt{3} \\ 3+\sqrt{3} & 0 \end{bmatrix} \in$ $\mathbf{SL}(2,\mathbb{R})$.



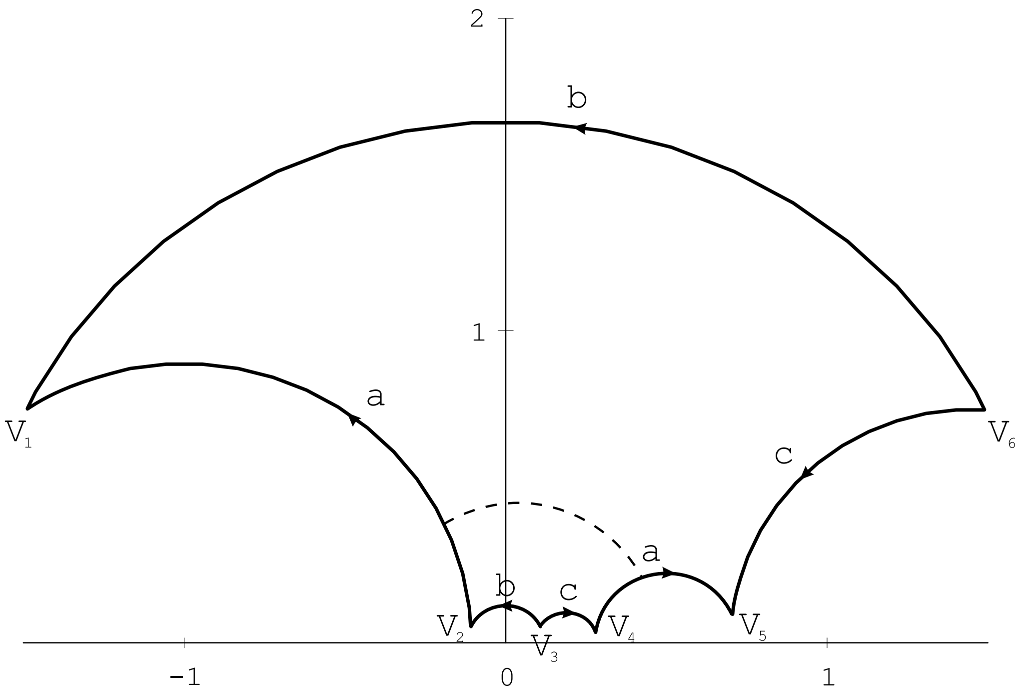
Fundamental domain for $X_6 := X(6,1)$

Elliptic cycles: $\{v_1, v_3, v_5\}, \{v_6\}, \{v_2\}, \{v_4\}$



Fundamental domain for $X_{10} := X(10, 1)$

Elliptic cycles of order 3: $\{v_1.v_3\}, \{v_4, v_6\}, \{v_2\}, \{v_5\}$



Fundamental domain for $X_{15} := X(15,1)$

Elliptic cycles of order 3: $\{v_1, v_2, v_4, v_5\}, \{v_3, v_6\}$

Moduli description of Shimura curves

$\Phi : H \hookrightarrow \mathbf{M}(2,\mathbb{R}), \quad \alpha^* := \mu^{-1}\overline{\alpha}\mu,\ \mu^2 = -D$ positive involution

$X(D,N)/\mathbb{Q}$ canonical model

$[(A, \iota, \mathcal{L}, G)]$

- A abelian surface

- $\iota : \mathcal{O}(D,1) \hookrightarrow \mathrm{End}(A),\ H \hookrightarrow \mathrm{End}^0(A) := \mathrm{End(A)} \otimes_{\mathbb{Z}} \mathbb{Q}$ QM

- $\mathcal{L}$ principal polarization on A whose Rosati involution in $\mathrm{End}^0(A)$ is compatible with the positive involution of $H : \alpha \to \alpha^*$

- $G \leq A[N]$, $\sharp G = N$ cyclic $\mathcal{O}(D,N)$-module

Complex multiplication points

$F = \mathbb{Q}(\sqrt{d}),\ d < 0$; $R(d,m)$ order of conductor m

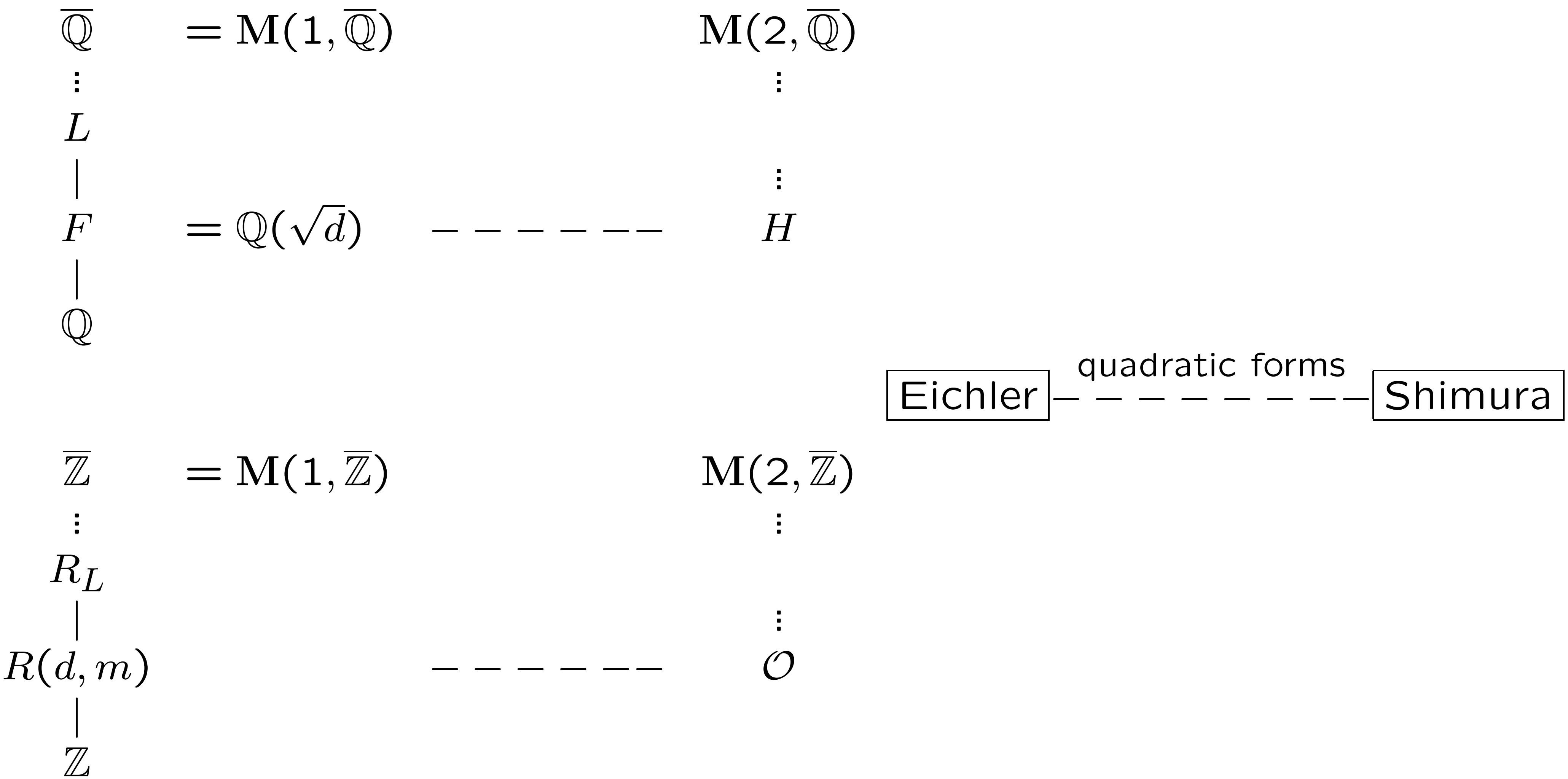
$[(A,\iota,\mathcal{L},G)]$ CM-point by $R(d,m) \Leftrightarrow \mathrm{End}(A,\iota,\mathcal{L},G) \simeq R(d,m)$

$\varphi : F \hookrightarrow H$, $H \otimes F \simeq \mathbf{M}(2,F)$, $\mathrm{End}^0(A,\iota,\mathcal{C},G) = \mathbf{M}(2,F)$

CM points generate class fields:

$z \in \mathcal{H}$ fixed by $\varphi(F^*)$, $j_{D,N}(\pi(z)) = [(A,i,\mathcal{C},G)] \in X(D,N)(F^{ab})$

- Shimura reciprocity law, 1959


$\overline{\mathbb{Q}}$
$= \mathbf{M}(1, \overline{\mathbb{Q}})$
$\mathbf{M}(2, \overline{\mathbb{Q}})$
L
F
$= \mathbb{Q}(\sqrt{d})$
H
$\mathbb{Q}$
Eichler
quadratic forms
Shimura
$\overline{\mathbb{Z}}$
$= \mathbf{M}(1, \overline{\mathbb{Z}})$
$\mathbf{M}(2, \overline{\mathbb{Z}})$
R_L
$R(d, m)$
$\mathcal{O}$
$\mathbb{Z}$

$X(D,N)$ Shimura curve $\varphi : R(d,m) \hookrightarrow \mathcal{O}(D,N)$

- $d > 0$, $\gamma \in \Gamma(D,N)$, hyperbolic transformations

- $d = -1, -3$, elliptic points

- $d < 0$, $d \neq -1, -3$, CM-points

embeddings $\longrightarrow$ Fundamental domain $\mathcal{D}(D,N)$
CM points
SCM points $n_{R(d,m),2} \to DN$

$\uparrow$

quadratic forms

Embeddings of quadratic orders into quaternion orders

$$\mathcal{O} \subseteq H, \qquad R \subseteq F = \mathbb{Q}(\sqrt{d})$$

$\mathcal{E}(\mathcal{O}, R) = \{\varphi : \varphi : R \hookrightarrow \mathcal{O} \text{ ring homomorphism}\}$

φ optimal $\Leftrightarrow \varphi(F) \cap \mathcal{O} = \varphi(R) \Leftrightarrow \varphi^{-1}(\varphi(F) \cap \mathcal{O}) = R$

$\mathcal{E}^*(\mathcal{O}, R) = \{\varphi : \varphi : R \hookrightarrow \mathcal{O} \text{ optimal}\}$

Quaternion algebras and quadratic forms

$f_n = \sum_{i=1}^{n} a_{ij} X_i X_j, \quad a_{ij} = a_{ji}$

$F = \mathbb{Q}(\sqrt{d})$, $\quad n_{F,2}(X,Y) = X^2 - dY^2$, $\quad \mathbb{Q}$-equivalence,

$R = R(d,m)$, $\quad n_{R,2}$, $\quad \mathbb{Z}$-equivalence;

$H = \left(\frac{a,b}{\mathbb{Q}}\right)$, $\quad n_{H,4} = X^2 - aY^2 - bZ^2 + abT^2$;

$H_0 = \langle i,j,k \rangle$, $\quad n_{H,3} = -aY^2 - bZ^2 + abT^2$, $\quad \mathbb{Q}$-equivalence;

$\mathcal{O}$ quaternion order, $\mathcal{B}$ normalized basis,

$n_{\mathcal{O},4}$, $\quad n_{\mathcal{O},3}$, $\quad \mathbb{Z}$-equivalence

$$\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathbf{M}(2, \mathbb{R}) \longrightarrow f_\gamma(X,Y) = cX^2 + (d-a)XY - bY^2$$

$$f = (A, B, C), \quad \mathcal{P}(f) := \{z : Az^2 + Bz + C = 0,\ \mathrm{Im}(z) \geq 0\}$$

• Let $z \in \mathcal{H}$. Then,

$$\gamma(z) = z \Leftrightarrow z \in \mathcal{P}(f_\gamma).$$

$$\det{}_1(f) := AC - B^2/4, \qquad \det{}_2(f) := 4AC - B^2$$

Binary forms attached to quaternion orders

$$\begin{array}{rcc} \Phi : H & \hookrightarrow & \mathbf{M}(2,\mathbb{R}) \\ \alpha = x + yi + zj + tk & \mapsto & \begin{bmatrix} x + y\sqrt{a} & z + t\sqrt{a} \\ b(z - t\sqrt{a}) & x - y\sqrt{a} \end{bmatrix} \end{array}$$

$$f_{\Phi(\alpha)} := (b(z - t\sqrt{a}), -2y\sqrt{a}, -z - t\sqrt{a})$$

$$\mathcal{H}(\mathcal{O}) := \{f_{\Phi(\alpha)} : \alpha \in \mathcal{O} \cap H_0\}$$

- $\mathcal{H}(\mathcal{O}_0(1,1)) = \{(a,\, 2b,\, c) : a, b, c \in \mathbb{Z}\}$

- $\mathcal{H}(\mathcal{O}_A(2p,1)) = \left\{(a + b\sqrt{p},\, 2c\sqrt{p},\, a - b\sqrt{p}) : a, b, c \in \mathbb{Z}\right\}$

- $\mathcal{H}(\mathcal{O}_B(pq,1)) = \left\{\frac{1}{2}(q(a + b\sqrt{p}),\, 2c\sqrt{p},\, -a + b\sqrt{p}) : a, b, c \in \mathbb{Z}, 2|a, 2|(b - c)\right\}$

Embeddings and binary quadratic forms

$$\mathcal{H}(\mathcal{O}, R) := \{f \in \mathcal{H}(\mathcal{O}) : \mathrm{det}_1(f) = -D_R\}$$

• $\mathcal{E}(\mathcal{O}, R) \longleftrightarrow \mathcal{H}(\mathbb{Z} + 2\mathcal{O}, R), \quad \varphi \mapsto f_{\Phi(\varphi(\sqrt{D_R}))}$

$\mathcal{R}(n_{\mathbb{Z}+2\mathcal{O},3}, -D_R; \mathbb{Z}) \longleftrightarrow \mathcal{H}(\mathbb{Z} + 2\mathcal{O}, R)$

• $\mathcal{E}(\mathcal{O}, R)^* \longleftrightarrow \mathcal{H}(\mathbb{Z} + 2\mathcal{O}, R)^*, \quad (\mathcal{O}, R)$-primitive binary

$\mathcal{R}(n_{\mathbb{Z}+2\mathcal{O},3}, -D_R; \mathbb{Z}) \longleftrightarrow \mathcal{H}(\mathbb{Z} + 2\mathcal{O}, R)$

Sets of primitive binary quadratic forms

- $\mathcal{H}^*(\mathbb{Z}+2\mathcal{O}_0(1,N),R) =$

$\{f = (Na, b, c) : a, b, c \in \mathbb{Z},\ \text{det}_2(f) = -D_R,\ \text{gcd}(a, b, c) = 1\}$

- $\mathcal{H}^*(\mathbb{Z}+2\mathcal{O}_A(2p,N),R) =$

$\{f = (a + b\sqrt{p}, 2c\sqrt{p}, a - b\sqrt{p}) : a, b, c \in \mathbb{Z},\ a \equiv b \equiv c \pmod 2,$

$N|(a+b),\ \text{det}_1(f) = -D_R,\ \text{gcd}\left(\frac{c+b}{2}, \frac{a+b}{2N}, b\right) = 1\}$

- $\mathcal{H}^*(\mathbb{Z}+2\mathcal{O}_B(pq,N),R) = \Big\{f = (q(a + b\sqrt{p}), 2c\sqrt{p}, -a + b\sqrt{p}) : a, b, c \in \mathbb{Z},$
$2N|(c-b),\ \text{gcd}\left(a, b, \frac{c-b}{2N}\right) = 1\Big\}$

Classes of primitive binary quadratic forms

$$\widetilde{\Phi} : \mathrm{Nor}(\mathcal{O}) \longrightarrow \{P \in \mathbf{GL}(2, \mathbb{R}) : \det P = \pm 1\}, \qquad G \leq \mathrm{Nor}(\mathcal{O}),$$

$$\Gamma_G := \widetilde{\Phi}(G) \leq \mathbf{GL}(2, \mathbb{R})$$

- $\mathcal{E}^*(\mathcal{O}, R)/G \longleftrightarrow \mathcal{H}^*(\mathbb{Z} + 2\mathcal{O}, R)/\Gamma_G$,

$H^*(\mathcal{O}, R; G) := \mathcal{H}^*(\mathbb{Z} + 2\mathcal{O}, R)/\Gamma_G$

$h(\mathcal{O}, R; G) := \# H^*(\mathcal{O}, R; G)$ cf. Eichler

Reduction theory

f semi-reduced $\Leftrightarrow \mathcal{P}(f) \subseteq \mathcal{D}(\overline{\Gamma}_G)$

f reduced

- Points with CM by R

$\{\mathcal{P}(f) : f \in \mathcal{H}^*(\mathbb{Z} + 2\mathcal{O}, R),\ f \text{ reduced}\}$

SCM-points

$F = \mathbb{Q}(\sqrt{d}) \qquad n_{F,2}(X,Y) = X^2 - dY^2$

$R = R(d,m) \qquad n_{R,2}(X,Y)$

$$n_{R,2}(X,Y) = \begin{cases} X^2 - \frac{D_F}{4} m^2 Y^2 & \text{if } D_F \equiv 0 \pmod 4 \\ X^2 + mXY + m^2 \frac{1 - D_F}{4} Y^2 & \text{if } D_F \equiv 1 \pmod 4 \end{cases}$$

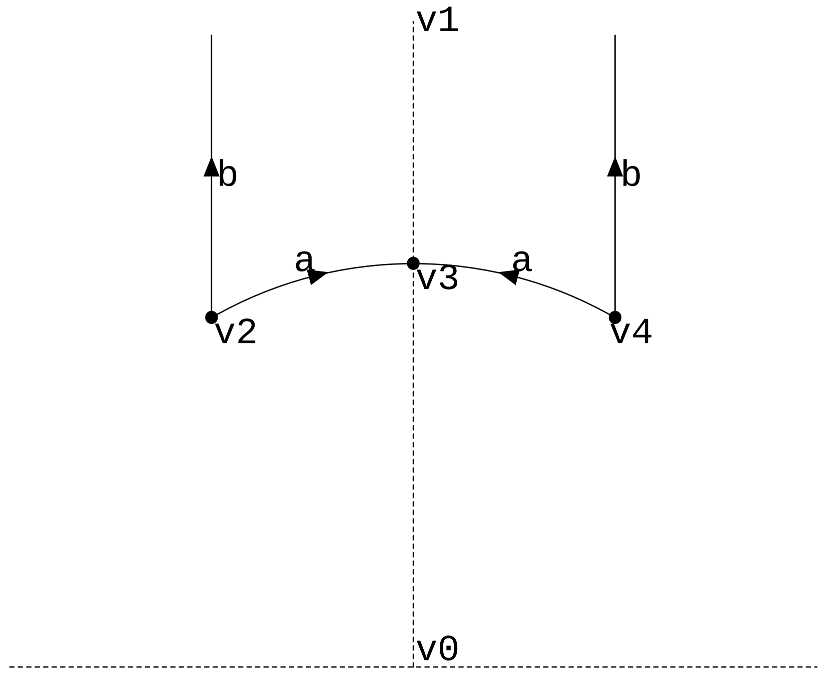
SCM points in $X(D,N)$:

$R(d,m) \hookrightarrow \mathcal{O}(D,N), \qquad n_{R(d,m),2}(X,Y) \to DN$

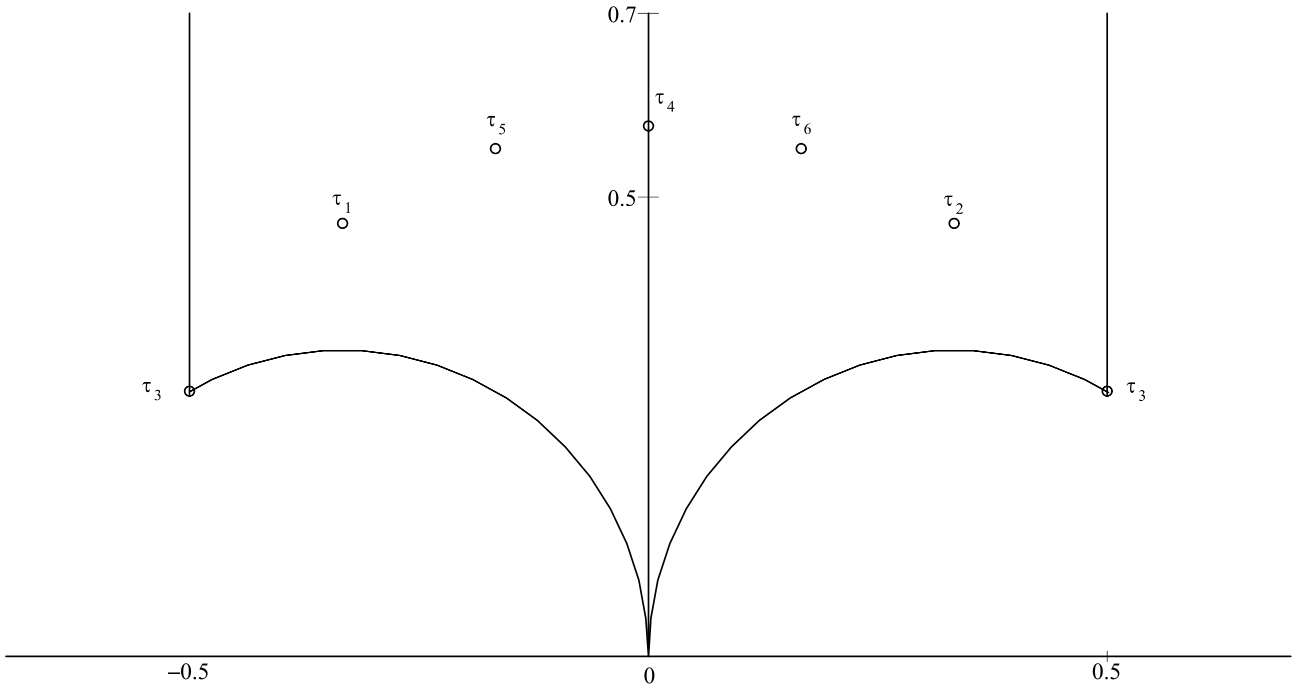
Special complex multiplication points are finite in number

SCM-points for $D = 6$

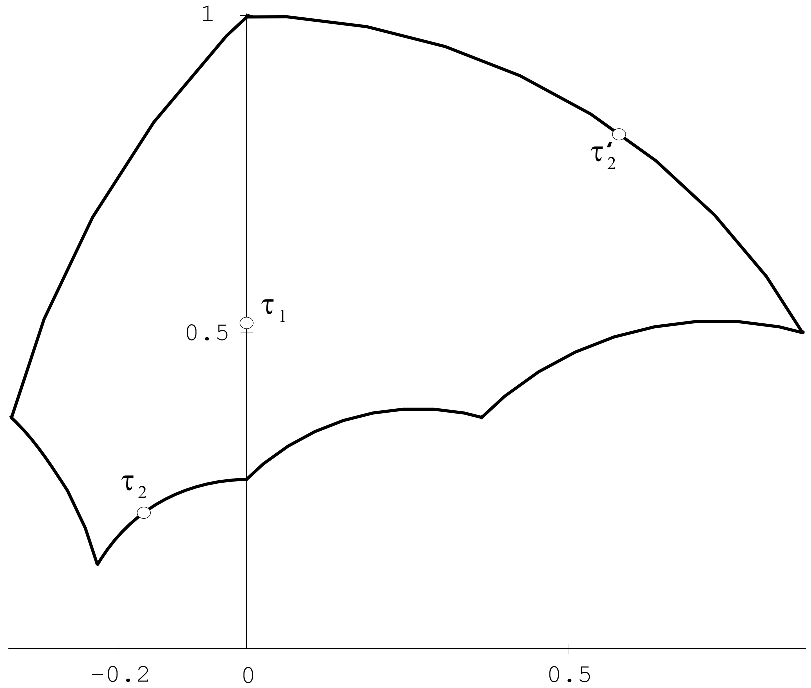
N	(d, m)	h	cm
1	(-6, 1)	2	2
	$\mathrm{scm}(6, 1) = 2$		
5	(-21, 1)	4	8
	(-30, 1)	4	4
	$\mathrm{scm}(6, 5) = 12$		
7	(-6, 1)	2	4
	(-33, 1)	4	8
	(-42, 1)	4	4
	$\mathrm{scm}(6, 7) = 16$		
11	(-30, 1)	4	8
	(-57, 1)	4	8
	(-66, 1)	8	8
	$\mathrm{scm}(6, 11) = 24$		
13	(-42, 1)	4	8
	(-69, 1)	8	16
	(-78, 1)	4	4
	$\mathrm{scm}(6, 13) = 28$		



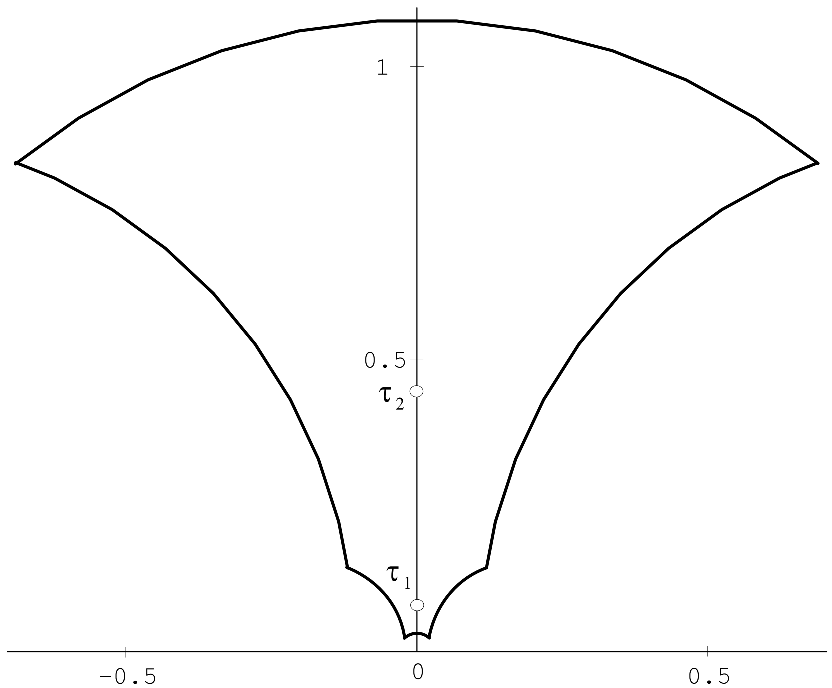
SCM-points in $X_0(1)$



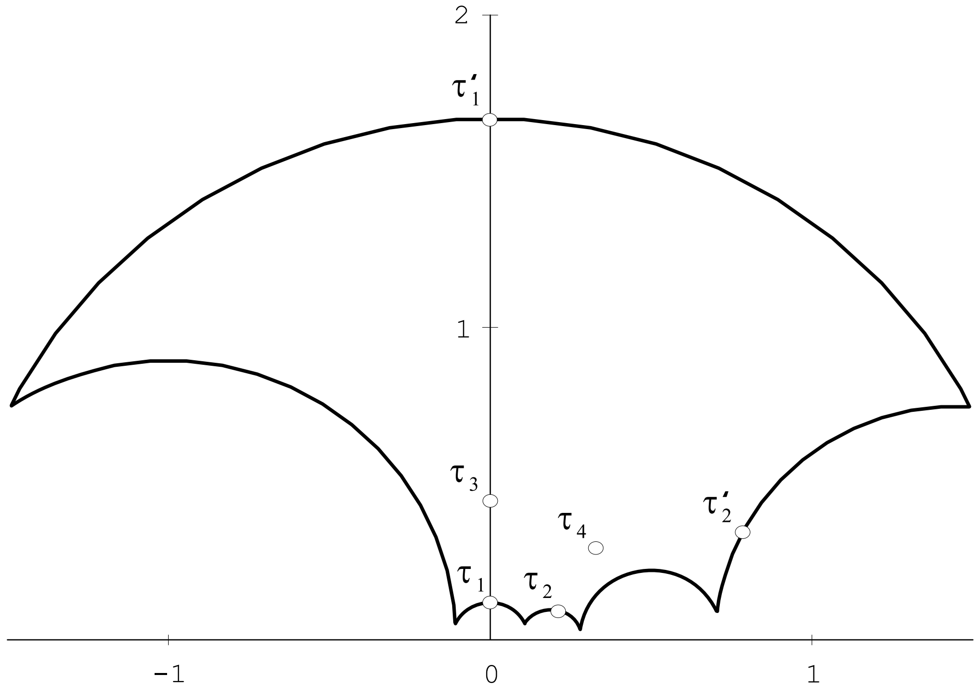
SCM-points in $X_0(3)$



SCM-points in X_6



SCM-points in X_{10}



SCM-points in X_{15}