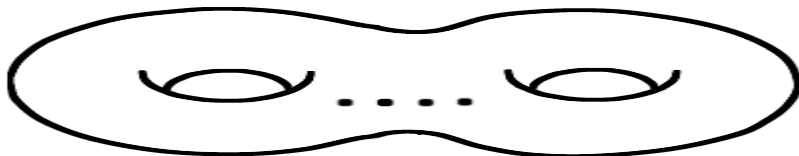


Genus 3 hyperelliptic curves with CM via Shimura Reciprocity

B. Dina, Ulm University, UPJV
S. Ionica, UPJV

ANTS 2020



Problem (Main Problem)

Let X be a hyperelliptic curve of genus 3 over \mathbb{C} with CM by K .
Compute the *Rosenhain class polynomials*

$$H_k^R(t) = \prod_{\sigma \in \text{Gal}(\mathcal{CM}(2)/K^r)} (t - \lambda_k^\sigma(X))$$

for $k = 1, \dots, 5$.

\rightsquigarrow The algorithmic solution is based on solutions of 3 subproblems.

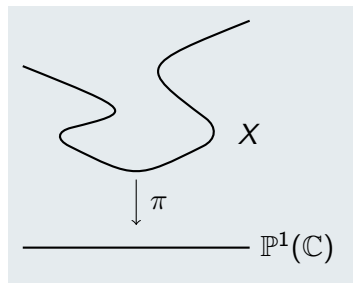
Previous work:

- Weng, 2005.
- Balakhrisnan, Ionica, Lauter, and Vincent, 2016.

Genus 3 hyperelliptic curves.

- Let $X : y^2 = f(x)$ be a hyperelliptic curve of genus 3 defined over \mathbb{C} , $\deg f = 7$.
- X is a cyclic covering of the projective line,

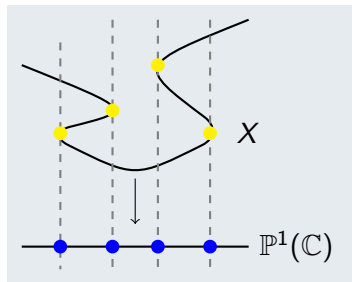
$$\pi : X \longrightarrow \mathbb{P}^1(\mathbb{C}), \deg(\pi) = 2.$$



Genus 3 hyperelliptic curves.

- Let $X : y^2 = f(x)$ be a hyperelliptic curve of genus 3 defined over \mathbb{C} , $\deg f = 7$.
- X is a cyclic covering of the projective line,

$$\pi : X \longrightarrow \mathbb{P}^1(\mathbb{C}), \deg(\pi) = 2.$$



- **Rosenhain form**

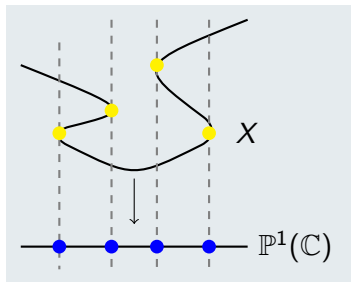
$$X : y^2 = x(x-1) \prod_{i=3}^7 (x - \lambda_i),$$

$\lambda_i \in \mathbb{C} \setminus \{0, 1\}$ pairwise distinct, $\lambda_\infty = \infty$.

Genus 3 hyperelliptic curves.

- Let $X : y^2 = f(x)$ be a hyperelliptic curve of genus 3 defined over \mathbb{C} , $\deg f = 7$.
- X is a cyclic covering of the projective line,

$$\pi : X \longrightarrow \mathbb{P}^1(\mathbb{C}), \deg(\pi) = 2.$$



- Rosenhain form

$$X : y^2 = x(x-1) \prod_{i=3}^7 (x-\lambda_i),$$

$$\lambda_i \in \mathbb{C} \setminus \{0, 1\} \text{ pairwise distinct, } \lambda_\infty = \infty.$$

The hyperelliptic Schottky Problem.

- $\mathcal{A}_3 = \mathrm{Sp}_6(\mathbb{Z}) \backslash \mathbb{H}_3$ the analytic moduli space of p.p.a.v. of dimension 3.
- $\mathcal{M}_3^{\mathrm{hyp}}$ = coarse moduli space of complex hyperelliptic curves of genus 3.

Problem (1)

Let $(A, E) \in \mathcal{A}_3$ be a simple moduli point with torus representation $A = \mathbb{C}^3 / (\mathbb{Z}^3 + Z\mathbb{Z}^3)$, $Z \in \mathbb{H}_3$. Are there $\alpha_i \in \mathbb{C}$ with $\alpha_i \neq \alpha_j$ for $i \neq j$ s.t. $X \in \mathcal{M}_3^{\mathrm{hyp}}$ given by

$$X : y^2 = \prod_{i \in \{1, 2, \dots, 7\}} (x - \alpha_i)$$

satisfies $(A, E) = (\mathrm{Jac}(X), \Theta)$.

Solution to Problem (1).

Let $Z \in \mathbb{H}_3$ be p.m. determining a simple point $(A, E) \in \mathcal{A}_3$. If

$\xi = \begin{pmatrix} \xi_1 \\ \xi_2 \end{pmatrix} \in (1/2)\mathbb{Z}^6$, then:

- ξ is **even theta characteristic**: $\xi_1 \cdot \xi_2 \equiv 0 \pmod{2}$.
- **Theta constant** = value of Riemann's theta-function

$$\vartheta[\xi](Z) = \vartheta[\xi](0, Z) = \sum_{n \in \mathbb{Z}^3} \exp(\pi i (n + \xi_1)^t Z (n + \xi_1) + 2\pi i (n + \xi_1)^t \xi_2).$$

Solution to Problem (1).

Let $Z \in \mathbb{H}_3$ be p.m. determining a simple point $(A, E) \in \mathcal{A}_3$. If

$\xi = \begin{pmatrix} \xi_1 \\ \xi_2 \end{pmatrix} \in (1/2)\mathbb{Z}^6$, then:

- ξ is **even theta characteristic**: $\xi_1 \cdot \xi_2 \equiv 0 \pmod{2}$.
- **Theta constant** = value of Riemann's theta-function

$$\vartheta[\xi](Z) = \vartheta[\xi](0, Z) = \sum_{n \in \mathbb{Z}^3} \exp(\pi i(n + \xi_1)^t Z(n + \xi_1) + 2\pi i(n + \xi_1)^t \xi_2)).$$

Theorem (Krazer)

Let $(A, E) \in \mathcal{A}_3$ be a simple moduli point with torus representation $A = \mathbb{C}^3 / (\mathbb{Z}^3 + Z\mathbb{Z}^3)$, $Z \in \mathbb{H}_3$ s.t. $(A, E) = (\text{Jac}(X), \Theta)$ for some $X \in \mathcal{M}_3^{\text{hyp}}$. Then

$$\#\{\vartheta[\xi](Z) \equiv 0 : \xi \text{ even theta characteristic}\} = 1.$$

Solution to Problem (1).

Let $Z \in \mathbb{H}_3$ be p.m. determining a simple point $(A, E) \in \mathcal{A}_3$. If

$\xi = \begin{pmatrix} \xi_1 \\ \xi_2 \end{pmatrix} \in (1/2)\mathbb{Z}^6$, then:

- ξ is **even theta characteristic**: $\xi_1 \cdot \xi_2 \equiv 0 \pmod{2}$.
- **Theta constant** = value of Riemann's theta-function

$$\vartheta[\xi](Z) = \vartheta[\xi](0, Z) = \sum_{n \in \mathbb{Z}^3} \exp(\pi i (n + \xi_1)^t Z (n + \xi_1) + 2\pi i (n + \xi_1)^t \xi_2).$$

Theorem (Krazer)

Let $(A, E) \in \mathcal{A}_3$ be a simple moduli point with torus representation $A = \mathbb{C}^3 / (\mathbb{Z}^3 + Z\mathbb{Z}^3)$, $Z \in \mathbb{H}_3$ s.t. $(A, E) = (\text{Jac}(X), \Theta)$ for some $X \in \mathcal{M}_3^{\text{hyp}}$. Then

$$\#\{\vartheta[\xi](Z) \equiv 0 : \xi \text{ even theta characteristic}\} = 1.$$

Moduli space with level 2-structure.

Every $Z \in \mathbb{H}_3$ determines triple (A, E, ν) :

- Abelian variety A represented by a torus

$$A = \mathbb{C}^3 / (\mathbb{Z}^3 + Z\mathbb{Z}^3)$$

+ principal polarization E .

- Symplectic isomorphism $\nu : A[2] \longrightarrow (\mathbb{Z}/2\mathbb{Z})^6$,

$$\frac{1}{2}(\xi_1 + Z\xi_2) \pmod{\mathbb{Z}^3 + Z\mathbb{Z}^3} \longmapsto \xi = \begin{pmatrix} \xi_1 \\ \xi_2 \end{pmatrix} \pmod{2}.$$

Moduli space with level 2-structure.

Every $Z \in \mathbb{H}_3$ determines triple (A, E, ν) :

- Abelian variety A represented by a torus

$$A = \mathbb{C}^3 / (\mathbb{Z}^3 + Z\mathbb{Z}^3)$$

+ principal polarization E .

- Symplectic isomorphism $\nu : A[2] \longrightarrow (\mathbb{Z}/2\mathbb{Z})^6$,

$$\frac{1}{2}(\xi_1 + Z\xi_2) \pmod{\mathbb{Z}^3 + Z\mathbb{Z}^3} \longmapsto \xi = \begin{pmatrix} \xi_1 \\ \xi_2 \end{pmatrix} \pmod{2}.$$

\rightsquigarrow Analytic moduli space of p.p.a.v. of dimension 3 with a level 2-structure:

$$\mathcal{A}_3[2] = \Gamma(2) \backslash \mathbb{H}_3.$$

Moduli space with level 2-structure.

Every $Z \in \mathbb{H}_3$ determines triple (A, E, ν) :

- Abelian variety A represented by a torus

$$A = \mathbb{C}^3 / (\mathbb{Z}^3 + Z\mathbb{Z}^3)$$

+ principal polarization E .

- Symplectic isomorphism $\nu : A[2] \longrightarrow (\mathbb{Z}/2\mathbb{Z})^6$,

$$\frac{1}{2}(\xi_1 + Z\xi_2) \pmod{\mathbb{Z}^3 + Z\mathbb{Z}^3} \longmapsto \xi = \begin{pmatrix} \xi_1 \\ \xi_2 \end{pmatrix} \pmod{2}.$$

\rightsquigarrow Analytic moduli space of p.p.a.v. of dimension 3 with a level 2-structure:

$$\mathcal{A}_3[2] = \Gamma(2) \backslash \mathbb{H}_3.$$

Solution based on Poor's Main Theorem

Azygetic system (a.s.): An ordered set $\eta = \{\eta_1, \dots, \eta_8\}$ of pairwise distinct characteristics, $\eta_i = \begin{pmatrix} \eta_{i1} \\ \eta_{i2} \end{pmatrix} \in (1/2)\mathbb{Z}^6$, $\eta_8 = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$ + some additional properties.

Poor's Main Theorem: For a moduli point $(A, E) \in \mathcal{A}_3$ with torus representation $A = \mathbb{C}^3/(\mathbb{Z}^3 + Z\mathbb{Z}^3)$, $Z \in \mathbb{H}_3$ are equivalent:

- A is simple and there is an a.s. η such that $\vartheta[\xi_\eta](Z) \equiv 0$.
- There is a moduli point $X \in \mathcal{M}_3^{hyp}$ satisfying the conditions of Problem (1), and

Solution based on Poor's Main Theorem

Azygetic system (a.s.): An ordered set $\eta = \{\eta_1, \dots, \eta_8\}$ of pairwise distinct characteristics, $\eta_i = \begin{pmatrix} \eta_{i1} \\ \eta_{i2} \end{pmatrix} \in (1/2)\mathbb{Z}^6$, $\eta_8 = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$ + some additional properties.

Poor's Main Theorem: For a moduli point $(A, E) \in \mathcal{A}_3$ with torus representation $A = \mathbb{C}^3/(\mathbb{Z}^3 + Z\mathbb{Z}^3)$, $Z \in \mathbb{H}_3$ are equivalent:

- A is simple and there is an a.s. η such that $\vartheta[\xi_\eta](Z) \equiv 0$.
- There is a moduli point $X \in \mathcal{M}_3^{hyp}$ satisfying the conditions of Problem (1), and
 - ▶ α_∞ corresponds to the basepoint P_0 of the Abel-Jacobi map

$$h_{P_0} : X \longmapsto \text{Jac}(X).$$

- ▶ The a.s. $\eta \pmod{2}$ describe the level 2-structure on X , i.e.
 $h_{P_0}(P_{\alpha_i}) = \nu^{-1}(\eta_i \pmod{2})$.

Solution based on Poor's Main Theorem

Azygetic system (a.s.): An ordered set $\eta = \{\eta_1, \dots, \eta_8\}$ of pairwise distinct characteristics, $\eta_i = \begin{pmatrix} \eta_{i1} \\ \eta_{i2} \end{pmatrix} \in (1/2)\mathbb{Z}^6$, $\eta_8 = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$ + some additional properties.

Poor's Main Theorem: For a moduli point $(A, E) \in \mathcal{A}_3$ with torus representation $A = \mathbb{C}^3/(\mathbb{Z}^3 + Z\mathbb{Z}^3)$, $Z \in \mathbb{H}_3$ are equivalent:

- A is simple and there is an a.s. η such that $\vartheta[\xi_\eta](Z) \equiv 0$.
- There is a moduli point $X \in \mathcal{M}_3^{hyp}$ satisfying the conditions of Problem (1), and
 - ▶ α_∞ corresponds to the basepoint P_0 of the Abel-Jacobi map

$$h_{P_0} : X \longmapsto \text{Jac}(X).$$

- ▶ The a.s. $\eta \pmod{2}$ describe the level 2-structure on X , i.e. $h_{P_0}(P_{\alpha_i}) = \nu^{-1}(\eta_i \pmod{2})$.

$$\rightsquigarrow X \in \mathcal{M}_3^{hyp}[2].$$

Solution based on Poor's Main Theorem

Azygetic system (a.s.): An ordered set $\eta = \{\eta_1, \dots, \eta_8\}$ of pairwise distinct characteristics, $\eta_i = \begin{pmatrix} \eta_{i1} \\ \eta_{i2} \end{pmatrix} \in (1/2)\mathbb{Z}^6$, $\eta_8 = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$ + some additional properties.

Poor's Main Theorem: For a moduli point $(A, E) \in \mathcal{A}_3$ with torus representation $A = \mathbb{C}^3/(\mathbb{Z}^3 + Z\mathbb{Z}^3)$, $Z \in \mathbb{H}_3$ are equivalent:

- A is simple and there is an a.s. η such that $\vartheta[\xi_\eta](Z) \equiv 0$.
- There is a moduli point $X \in \mathcal{M}_3^{hyp}$ satisfying the conditions of Problem (1), and
 - ▶ α_∞ corresponds to the basepoint P_0 of the Abel-Jacobi map

$$h_{P_0} : X \longmapsto \text{Jac}(X).$$

- ▶ The a.s. $\eta \pmod{2}$ describe the level 2-structure on X , i.e. $h_{P_0}(P_{\alpha_i}) = \nu^{-1}(\eta_i \pmod{2})$.

$$\rightsquigarrow X \in \mathcal{M}_3^{hyp}[2].$$

Problem (2)

Let $(A, E, \nu) \in \mathcal{A}_3[2]$ be a simple moduli point with torus representation $A = \mathbb{C}^3/(\mathbb{Z}^3 + Z\mathbb{Z}^3)$, $Z \in \mathbb{H}_3$ s.t. $(A, E) = (\text{Jac}(X), \Theta)$ for a point $X \in \mathcal{M}_3^{\text{hyp}}[2]$ with

$$X : y^2 = \prod_{i=1}^7 (x - \alpha_i).$$

Compute the Rosenhain invariants of X .

Takase, Vincent: For $k = 1, \dots, 5$

$$\lambda_k = \exp(4\pi i(\eta_k + \eta_7)_1(\eta_6)_2) \left(\frac{\vartheta[c_1(\eta)]\vartheta[c_2(\eta)]}{\vartheta[c_3(\eta)]\vartheta[c_4(\eta)]} \right)^2 (Z).$$

$$X : y^2 = x(x-1) \prod_{i=3}^7 (x - \lambda_i).$$

Problem (2)

Let $(A, E, \nu) \in \mathcal{A}_3[2]$ be a simple moduli point with torus representation $A = \mathbb{C}^3/(\mathbb{Z}^3 + Z\mathbb{Z}^3)$, $Z \in \mathbb{H}_3$ s.t. $(A, E) = (\text{Jac}(X), \Theta)$ for a point $X \in \mathcal{M}_3^{\text{hyp}}[2]$ with

$$X : y^2 = \prod_{i=1}^7 (x - \alpha_i).$$

Compute the Rosenhain invariants of X .

Takase, Vincent: For $k = 1, \dots, 5$

$$\lambda_k = \exp(4\pi i(\eta_k + \eta_7)_1(\eta_6)_2) \left(\frac{\vartheta[c_1(\eta)]\vartheta[c_2(\eta)]}{\vartheta[c_3(\eta)]\vartheta[c_4(\eta)]} \right)^2 (Z).$$

$$X : y^2 = x(x-1) \prod_{i=3}^7 (x - \lambda_i).$$

Shimura's CM-Theory.

- Primitive CM pair (K, Φ) .
- Ideal $2\mathcal{O}_K$.
- Reflex pair (K^r, Φ^r) .
- Ray class group $Cl_{2\mathcal{O}_{K^r}}(K^r)$.

Shimura's CM-Theory.

- Primitive CM pair (K, Φ) .
- Ideal $2\mathcal{O}_K$.
- $\text{Princ}(K, \Phi, 2)$ = set of p.p.a.v. with CM by K , fixed Φ , and a proper 2-t.p.
- Reflex pair (K^r, Φ^r) .
- Ray class group $Cl_{2\mathcal{O}_{K^r}}(K^r)$.
- $\frac{I_{2\mathcal{O}_{K^r}}(K^r)}{H_{2\mathcal{O}_{K^r}}(K^r)} \cong \text{Gal}(\mathcal{CM}(2)/K^r)$.

Shimura's CM-Theory.

- Primitive CM pair (K, Φ) .
- Ideal $2\mathcal{O}_K$.
- $\text{Princ}(K, \Phi, 2)$ = set of p.p.a.v. with CM by K , fixed Φ , and a proper 2-t.p.
- Reflex pair (K^r, Φ^r) .
- Ray class group $Cl_{2\mathcal{O}_{K^r}}(K^r)$.
- $\frac{I_{2\mathcal{O}_{K^r}}(K^r)}{H_{2\mathcal{O}_{K^r}}(K^r)} \cong \text{Gal}(\mathcal{CM}(2)/K^r)$.

Shimura's CM-action: For $A = A(\mathfrak{a}, \xi, t) \in \text{Princ}(K, \Phi, 2)$ and $[\mathfrak{c}_\sigma] \in \frac{I_{2\mathcal{O}_{K^r}}(K^r)}{H_{2\mathcal{O}_{K^r}}(K^r)}$ corresponding to $\sigma \in \text{Gal}(\mathcal{CM}(2)/K^r)$

$$\rightsquigarrow A^{\mathfrak{c}_\sigma} = A(N_{\Phi^r}(\mathfrak{c}_\sigma)^{-1}\mathfrak{a}, N_{K^r/\mathbb{Q}}(\mathfrak{c}_\sigma)\xi, t \mod (N_{\Phi^r}(\mathfrak{c}_\sigma)^{-1}\mathfrak{a})).$$

Shimura's CM-Theory.

- Primitive CM pair (K, Φ) .
- Ideal $2\mathcal{O}_K$.
- $\text{Princ}(K, \Phi, 2)$ = set of p.p.a.v. with CM by K , fixed Φ , and a proper 2-t.p.
- Reflex pair (K^r, Φ^r) .
- Ray class group $Cl_{2\mathcal{O}_{K^r}}(K^r)$.
- $\frac{I_{2\mathcal{O}_{K^r}}(K^r)}{H_{2\mathcal{O}_{K^r}}(K^r)} \cong \text{Gal}(\mathcal{CM}(2)/K^r)$.

Shimura's CM-action: For $A = A(\mathfrak{a}, \xi, t) \in \text{Princ}(K, \Phi, 2)$ and $[\mathfrak{c}_\sigma] \in \frac{I_{2\mathcal{O}_{K^r}}(K^r)}{H_{2\mathcal{O}_{K^r}}(K^r)}$ corresponding to $\sigma \in \text{Gal}(\mathcal{CM}(2)/K^r)$

$$\rightsquigarrow A^{\mathfrak{c}_\sigma} = A(N_{\Phi^r}(\mathfrak{c}_\sigma)^{-1}\mathfrak{a}, N_{K^r/\mathbb{Q}}(\mathfrak{c}_\sigma)\xi, t \mod (N_{\Phi^r}(\mathfrak{c}_\sigma)^{-1}\mathfrak{a})).$$

Problem (3)

Let $(A, E, \nu) \in \mathcal{A}_3[2]$ be a simple moduli point with:

- Torus representation $A = \mathbb{C}^3 / (\mathbb{Z}^3 + Z\mathbb{Z}^3)$ with $Z \in \mathbb{H}_3$.
- $(A, E) = (\text{Jac}(X), \Theta)$, $X \in \mathcal{M}_3^{\text{hyp}}[2]$ in Rosenhain form.
- Let η be an a.s. for Z .

For $[\mathfrak{c}_\sigma] \in \frac{I_2 \mathcal{O}_{K^r}(K^r)}{H_2 \mathcal{O}_{K^r}(K^r)}$ corresponding to $\sigma \in \text{Gal}(\mathcal{CM}(2)/K^r)$ compute:

- The Rosenhain invariants of $X^\sigma \in \mathcal{M}_3^{\text{hyp}}[2]$ with $(\text{Jac}(X^\sigma), \Theta^\sigma) = (A^{\mathfrak{c}_\sigma}, E^{\mathfrak{c}_\sigma})$.
- The conjugate a.s. η^σ for $Z' \in \mathbb{H}_3$ corresponding to $A^{\mathfrak{c}_\sigma}$.

Problem (3)

Let $(A, E, \nu) \in \mathcal{A}_3[2]$ be a simple moduli point with:

- Torus representation $A = \mathbb{C}^3 / (\mathbb{Z}^3 + Z\mathbb{Z}^3)$ with $Z \in \mathbb{H}_3$.
- $(A, E) = (\text{Jac}(X), \Theta)$, $X \in \mathcal{M}_3^{\text{hyp}}[2]$ in Rosenhain form.
- Let η be an a.s. for Z .

For $[\mathfrak{c}_\sigma] \in \frac{I_{2\mathcal{O}_{K^r}}(K^r)}{H_{2\mathcal{O}_{K^r}}(K^r)}$ corresponding to $\sigma \in \text{Gal}(\mathcal{CM}(2)/K^r)$ compute:

- The Rosenhain invariants of $X^\sigma \in \mathcal{M}_3^{\text{hyp}}[2]$ with $(\text{Jac}(X^\sigma), \Theta^\sigma) = (A^{\mathfrak{c}_\sigma}, E^{\mathfrak{c}_\sigma})$.
- The conjugate a.s. η^σ for $Z' \in \mathbb{H}_3$ corresponding to $A^{\mathfrak{c}_\sigma}$.

Solution to Problem (3).

- Our solution is based on Streng's effective formulation of Shimura's Reciprocity Law.
- For every $[\mathfrak{c}_\sigma] \in \frac{I_2 \mathcal{O}_{K^r}(K^r)}{H_2 \mathcal{O}_{K^r}(K^r)}$ corresponding to $\sigma \in \text{Gal}(\mathcal{CM}(2)/K^r)$ there are matrices $M \in \text{GSp}_6(\mathbb{Q})$, $U \in \text{Sp}_6(\mathbb{Z}/2\mathbb{Z})$ s.t.

$$\lambda_i^\sigma(Z) = \lambda_i^U(M.Z).$$

Solution to Problem (3).

- Our solution is based on Streng's effective formulation of Shimura's Reciprocity Law.
- For every $[\mathfrak{c}_\sigma] \in \frac{I_{2\mathcal{O}_{K^r}}(K^r)}{H_{2\mathcal{O}_{K^r}}(K^r)}$ corresponding to $\sigma \in \text{Gal}(\mathcal{CM}(2)/K^r)$ there are matrices $M \in \text{GSp}_6(\mathbb{Q})$, $U \in \text{Sp}_6(\mathbb{Z}/2\mathbb{Z})$ s.t.

$$\lambda_i^\sigma(Z) = \lambda_i^U(M.Z).$$

- After some linear transformations on $M.Z \rightsquigarrow Z' \in \mathbb{H}_3$ s.t.
 - ▶ $\eta^\sigma = \eta$ is the conjugate a.s. attach to Z' .
 - ▶ $\lambda_i^\sigma(Z) = \lambda_i(Z')$.

Solution to Problem (3).

- Our solution is based on Streng's effective formulation of Shimura's Reciprocity Law.
- For every $[\mathfrak{c}_\sigma] \in \frac{I_{2\mathcal{O}_{K^r}}(K^r)}{H_{2\mathcal{O}_{K^r}}(K^r)}$ corresponding to $\sigma \in \text{Gal}(\mathcal{CM}(2)/K^r)$ there are matrices $M \in \text{GSp}_6(\mathbb{Q})$, $U \in \text{Sp}_6(\mathbb{Z}/2\mathbb{Z})$ s.t.

$$\lambda_i^\sigma(Z) = \lambda_i^U(M.Z).$$

- After some linear transformations on $M.Z \rightsquigarrow Z' \in \mathbb{H}_3$ s.t.
 - ▶ $\eta^\sigma = \eta$ is the conjugate a.s. attach to Z' .
 - ▶ $\lambda_i^\sigma(Z) = \lambda_i(Z')$.

Thank you for listening!