Isogenous hyperelliptic and non-hyperelliptic Jacobians with maximal Complex Multiplication

Joint work with
S. Ionica (UPJV), and J. Sijsling (Ulm University).

Outline I

1. The main objects.
   - CM fields and their CM types.
   - The Galois group of a CM field.
   - Abelian varieties, and algebraic curves.
   - The Jacobian of an algebraic curve.

2. A brief introduction in Complex Multiplication (CM) Theory.
   - The main idea of CM Theory.
   - Principally polarized abelian varieties with CM by $\mathbb{Z}_K$.
     - The construction of p.p.a.v. with CM by $\mathbb{Z}_K$.

Outline II

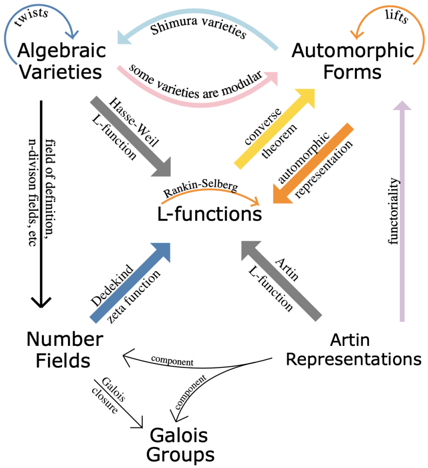
3. The project.
   - Motivation
   - The goal.
   - Main Result 1.
   - Main Result 2.
   - Main Result 3.

4. The computation of the sets $\mathcal{M}_{\mathbb{Z}_K}$ and $\mathcal{M}_{\mathbb{Z}_K}(\Phi)$.
   - The sets $\mathcal{M}_{\mathbb{Z}_K}$ and $\mathcal{M}_{\mathbb{Z}_K}(\Phi)$.
   - The Shimura class group $\mathcal{C}_K$ and its reflex type norm subgroup.
   - The precomputation step.
   - The algorithms.

The L-functions and Modular Forms Database.

The L-functions and Modular Forms Database (LMFDB).

- What is the LMFDB?
- The importance of the LMFDB in Mathematics?
- The objects in today's discussion:
    - Complex Multiplication (CM) fields and their
    - Galois groups.
    - Algebraic curves and their
    - Jacobians.



1. The objects in today's discussion

Complex Multiplication (CM) fields, and their CM types.

- A CM field K is a totally imaginary quadratic extension of a totally real number field K_0.
- Let L be the Galois closure of K. A CM type Φ on K (with values in L) is a subset $\Phi \subset \mathrm{Hom}(K, L)$ such that
$$\mathrm{Hom}(K, L) = \Phi \amalg \overline{\Phi}.$$
- The reflex field $K^r \subset L$ of (K, Φ) is the fixed field of the group $H = \{\sigma \in \mathrm{Gal}(L|\mathbb{Q}) : \sigma\Phi_L = \Phi_L\}$.
- The reflex CM type Φ^r of K^r is induced by the CM type Φ_L^{-1} on L.

2. The objects in today's discussion

The Galois group of a sextic CM field.

Theorem

Let K be sextic CM field, with Galois closure L. Then $G = \mathrm{Gal}(L|\mathbb{Q})$ is isomorphic to one of the following groups:

1. C_6.
2. D_6.
3. $C_2^3 \rtimes C_3$.
4. $C_2^3 \rtimes S_3$.

3. The objects in today's discussion

- Our fields K are all algebraically closed and of characteristic zero.
- All our curves over a field K are separated and geometrically integral schemes of dimension 1 over K.
- The genus:
  - $g = 1$: Elliptic curves.
  - $g = 2$: Hyperelliptic curves.
  - $g = 3$: Hyperelliptic curves, and quartic plane curves.
- An abelian variety over K is an algebraic group that is geometrically integral and proper over K.

4. The objects in today's discussion

The Jacobian $\mathrm{Jac}(X)$ of a curve X over $\mathbb{C}$.

- We can compute the Jacobian of X in the following way:
  - Let γ_i be a basis for the homology group $H_1(X, \mathbb{Z}) \cong \mathbb{Z}^{2g}$.
  - Let $\omega_1, \ldots, \omega_g$ be a basis of differential forms on X.
  - Compute the vectors $\lambda_i \in \mathbb{C}^g$ for all $i = 1, \ldots, 2g$ by

$$(\lambda_i)_j = \int_{\gamma_j} \omega_i.$$

  - Then $\Lambda = \langle \lambda_1, \ldots, \lambda_{2g} \rangle$ is a lattice in $\mathbb{C}^g$ called the period lattice of X.
  - Define

$$\mathrm{Jac}(X) = \mathbb{C}^g / \Lambda.$$

1. The main idea of CM Theory.

Motivation: Is there a way to describe a general method for describing all Abelian extensions of a number field?

- The Kronecker-Weber Theorem: Any abelian extension $\mathbb{Q} \subset L$ is contained in some cyclotomic fields $\mathbb{Q}(\zeta_n)$ for some n, $\zeta_n = \exp(2\pi i/n)$.
- Kronecker's Jugendtraum (Hilbert 12): Replacing $\mathbb{Q}$ by a different base field K, and ζ_n by some „complex numbers", is there a statement that is analogous to the Kronecker-Weber Theorem?

2. The main idea of CM Theory.

The answer to Kronecker's Jugendtraum is given by:

- The theory of Complex Multiplication (CM) introduced by Shimura and *Taniyama* in the 1950's.
- Complete answer to Kronecker's Jugendtraum in the case of CM fields.

3. The main idea of CM Theory.

The genus one case.

Theorem (Main Theorem 1)

Let K be an imaginary quadratic field with ring of integers $\mathbb{Z}_K$, and let E be an elliptic curve over $\mathbb{C}$ with $\mathrm{End}(E) \cong \mathbb{Z}_K$. *Then $j(E)$ is an algebraic integer, and*

$$K(j(E))$$

is the Hilbert class field H of K.

Theorem

If H is the Hilbert class field of K, then the Artin map $I_K \to \mathrm{Gal}(H|K)$ is surjective and induces an isomorphism

$$Cl(K) \xrightarrow{\sim} \mathrm{Gal}(H|K).$$

Principally polarized abelian abelian varieties (p.p.a.v) with CM by $\mathbb{Z}_K$.

Theorem

Simple principally polarized abelian varieties of dimension three are Jacobian varieties.

Definition

Let K be a sextic CM field. A principally polarized abelian variety A of dimension three has CM by the maximal order $\mathbb{Z}_K$ if $\mathrm{End}(A) \cong \mathbb{Z}_K$.

1. The construction of p.p.a. varieties with CM by $\mathbb{Z}_K$

The dimension one case:

- An imaginary quadratic field K with ring of integers $\mathbb{Z}_K$.
- A fractional $\mathbb{Z}_K$-ideal $\mathfrak{a}$.

The dimension three case:

- An sextic CM field K with ring of integers $\mathbb{Z}_K$.
- A fractional $\mathbb{Z}_K$-ideal $\mathfrak{a}$.

1. The construction of p.p.a. varieties with CM by $\mathbb{Z}_K$

The dimension one case:

- An imaginary quadratic field K with ring of integers $\mathbb{Z}_K$.
- A fractional $\mathbb{Z}_K$-ideal $\mathfrak{a}$.
- There exists a correspondence between $[\mathfrak{a}] \in Cl(K)$ and lattice $\Lambda \subset \mathbb{C}$ modulo equivalence.

$\rightsquigarrow E \cong \mathrm{Jac}(E)$.

The dimension three case:

- An sextic CM field K with ring of integers $\mathbb{Z}_K$.
- A fractional $\mathbb{Z}_K$-ideal $\mathfrak{a}$.
- Together with a primitive CM type Φ of K, there exists correspondence between $[\mathfrak{a}] \in Cl(K)$ and lattice $\Lambda = \Phi(\mathfrak{a}) \subset \mathbb{C}^3$ modulo equivalence.

$\rightsquigarrow A \cong \mathbb{C}^3/\Lambda$.

1. The construction of p.p.a. varieties with CM by $\mathbb{Z}_K$

The dimension one case:

- An imaginary quadratic field K with ring of integers $\mathbb{Z}_K$.
- A fractional $\mathbb{Z}_K$-ideal $\mathfrak{a}$.
- There exists a correspondence between $[\mathfrak{a}] \in Cl(K)$ and lattice $\Lambda \subset \mathbb{C}$ modulo equivalence.

$\rightsquigarrow E \cong \mathrm{Jac}(E)$.

The dimension three case:

- An sextic CM field K with ring of integers $\mathbb{Z}_K$.
- A fractional $\mathbb{Z}_K$-ideal $\mathfrak{a}$.
- Together with a primitive CM type Φ of K, there exists correspondence between $[\mathfrak{a}] \in Cl(K)$ and lattice $\Lambda = \Phi(\mathfrak{a}) \subset \mathbb{C}^3$ modulo equivalence.

$\rightsquigarrow A \cong \mathbb{C}^3/\Lambda$.

2. The construction of p.p.a. varieties with CM by $\mathbb{Z}_K$

Principal polarization in the dimension three case.

- Ket $\xi \in K$, such that $-\xi^2$ is totally positive in K_0, and $\operatorname{im}(\varphi(\xi)) > 0$ for all $\varphi \in \Phi$, and such that $(\xi) = (\mathfrak{a}\overline{\mathfrak{a}}\mathfrak{D}_{K|\mathbb{Q}})^{-1}$.
- Then $(\Phi, \mathfrak{a}, \xi)$ gives rise to a p.p.a.v

$$A(\mathfrak{a}, \xi) \cong (\mathbb{C}^3/\Lambda, E)$$

of dimension three over $\mathbb{C}$, with

- Principal polarization $E(\Phi(\alpha), \Phi(\beta)) := \mathrm{Tr}_{K|\mathbb{Q}}(\xi\overline{\alpha}\beta)$ for $\alpha, \beta \in K$, and
- Where $A(\mathfrak{a}, \xi)$ has CM by $\mathbb{Z}_K$.

Motivation.

Motivation:

- In the genus three case there are two types of curves, hyperelliptic curves, and quartic plane curves.
- By the André-Oort conjecture the number of hyperelliptic curves with CM over $\mathbb{C}$ might be finite.

Motivation.

Motivation:

- In the genus three case there are two types of curves, hyperelliptic curves, and quartic plane curves.
- By the André-Oort conjecture the number of hyperelliptic curves with CM over $\mathbb{C}$ might be finite.
- Is there any sextic CM field K in the LMFDB with $\mathbb{Q}(i) \notin K$, for which there exists a hyperelliptic curve whose Jacobian has primitive CM by $\mathbb{Z}_K$?

Motivation.

Motivation:

- In the genus three case there are two types of curves, hyperelliptic curves, and quartic plane curves.
- By the André-Oort conjecture the number of hyperelliptic curves with CM over $\mathbb{C}$ might be finite.
- Is there any sextic CM field K in the LMFDB with $\mathbb{Q}(i) \notin K$, for which there exists a hyperelliptic curve whose Jacobian has primitive CM by $\mathbb{Z}_K$?
- Cryptographic relevance. Is there any sextic CM field K in the LMFDB for which there exists a hyperelliptic curve X and a quartic plane curve Y whose Jacobian has primitive CM by $\mathbb{Z}_K$?

Motivation.

Motivation:

- In the genus three case there are two types of curves, hyperelliptic curves, and quartic plane curves.
- By the André-Oort conjecture the number of hyperelliptic curves with CM over $\mathbb{C}$ might be finite.
- Is there any sextic CM field K in the LMFDB with $\mathbb{Q}(i) \notin K$, for which there exists a hyperelliptic curve whose Jacobian has primitive CM by $\mathbb{Z}_K$?
- Cryptographic relevance. Is there any sextic CM field K in the LMFDB for which there exists a hyperelliptic curve X and a quartic plane curve Y whose Jacobian has primitive CM by $\mathbb{Z}_K$?
- If yes, does there exist an isogeny of small degree between the Jacobian of X and Y, where both Jacobians have CM by $\mathbb{Z}_K$?

Motivation.

Motivation:

- In the genus three case there are two types of curves, hyperelliptic curves, and quartic plane curves.
- By the André-Oort conjecture the number of hyperelliptic curves with CM over $\mathbb{C}$ might be finite.
- Is there any sextic CM field K in the LMFDB with $\mathbb{Q}(i) \notin K$, for which there exists a hyperelliptic curve whose Jacobian has primitive CM by $\mathbb{Z}_K$?
- Cryptographic relevance. Is there any sextic CM field K in the LMFDB for which there exists a hyperelliptic curve X and a quartic plane curve Y whose Jacobian has primitive CM by $\mathbb{Z}_K$?
- If yes, does there exist an isogeny of small degree between the Jacobian of X and Y, where both Jacobians have CM by $\mathbb{Z}_K$?

The goal.

A systematic search in the LMFDB with the aim to find:

- All sextic complex multiplication (CM) fields K for which (heuristically) there exist both hyperelliptic and non-hyperelliptic curves whose Jacobian has primitive CM by $\mathbb{Z}_K$.
- All sextic CM fields K for which (heuristically) there exists a hyperelliptic curve whose Jacobian has primitive CM by $\mathbb{Z}_K$?

Main Result 1

Main Result 1

Heuristically, there are 14 sextic CM fields K in the LMFDB for which there exist both a hyperelliptic and a non-hyperelliptic curve whose Jacobian has primitive CM by $\mathbb{Z}_K$. For all of these fields K we have that $\mathrm{Gal}(K\,|\,\mathbb{Q}) \simeq C_2^3 \rtimes S_3$.

Why are the fields from Main Result 1 interesting?

Cryptographic relevance:

- Solving the Discrete Logarithm Problem (DLP) in Jacobians of hyperelliptic curves of genus 3 in $\widetilde{O}(q^{4/3})$ using [GTTD07].
- Solving the DLP in Jacobians of non-hyperelliptic curves of genus 3 $\widetilde{O}(q)$ using [Die06].

Main Result 2

Main Result 2

Heuristically, including the fields mentioned in Main Result 1, there are $3,422$ CM fields K in the LMFDB for which there exists a hyperelliptic curve whose Jacobian has primitive CM by $\mathbb{Z}_K$. Of these fields,

- *348 have Galois group isomorphic to C_6.*
- *3,057 have Galois group isomorphic to D_6.*
- *17 have Galois group isomorphic to $C_2^3 \rtimes S_3$.*
- *We have $\mathbb{Q}(i) \subset K$ for all but 5 of these fields K, of which 2 (resp. 3) have Galois group isomorphic to C_6 (resp. $C_2^3 \rtimes S_3$).*

Main Result 2

Why are the fields from Main Result 2 interesting?

- By the André-Oort conjecture the number of hyperelliptic curves with CM over $\mathbb{C}$ might be finite.
- By [Wen01]: If $\mathrm{Jac}(X)$ is simple of dimension 3 and has CM by $\mathbb{Z}_K$, where $\mathbb{Q}(i) \subset K$, then X is hyperelliptic.
- [Kı16] classifies in her PhD thesis all $\mathbb{Q}(i) \subset K$ with $h_K = 1$ where there exists a hyperelliptic curve whose Jacobian has primitive CM by $\mathbb{Z}_K$.

Main Result 2

The exceptional case where $\mathbb{Q}(i) \notin K$ is from interest.

- The two fields with Galois group isomorphic to C_6 were already known by [BILV16].
- The three cases with Galois group isomorphic to $C_2^3 \rtimes S_3$ are completely new.

Main Result 3

Main Result 3

Let K be the CM field defined by the polynomial $t^6 + 10t^4 + 21t^2 + 4$, $d_K = -1 \cdot 2^8 \cdot 359^2$, and let r be a zero of the polynomial $t^4 - 5t^2 - 2t + 1$.

- *Consider the hyperelliptic curve*

$$\begin{aligned} X: \quad y^2 = {} & x^8+(-28r^3-4r^2+132r+84)x^7+(-600r^3-160r^2+2920r+2044)x^6 \\ & +(-3532r^3-940r^2+17224r+11944)x^5+(9040r^3+2890r^2-44860r-31460)x^4 \\ & +(167536r^3+49480r^2-824532r-576212)x^3 \\ & +(-226976r^3-64932r^2+1113648r+776872)x^2 \\ & +(-244204r^3-69572r^2+1197716r+835300)x \\ & +(319956r^3+94725r^2-1575062r-1100801), \end{aligned}$$

and

Main Result 3

- The smooth plane quartic curve

$$
\begin{aligned}
Y: \quad & (14106r^3-150652r^2+185086r+292255)x^4 \\
& +(-171112r^3+44200r^2+916008r+93360)x^3y \\
& +(-120788r^3+49032r^2+382244r+300708)x^3z \\
& +(467744r^3-209864r^2-2160704r+183416)x^2y^2 \\
& +(-72248r^3+64768r^2+347488r-362984)x^2yz \\
& +(5720r^3-12378r^2-15628r+50692)x^2z^2 \\
& +(-512608r^3+349824r^2+2423616r-580448)xy^3 \\
& +(202192r^3-151024r^2-1180320r+403568)xy^2z \\
& +(6512r^3-11272r^2+178120r-71336)xyz^2+(-11832r^3+12268r^2-844r+1376)xz^3 \\
& +(263424r^3-176880r^2-1159232r+335040)y^4 \\
& +(-201216r^3+100448r^2+856096r-249632)y^3z \\
& +(62112r^3+1984r^2-226512r+71624)y^2z^2\cdots
\end{aligned}
$$

Main Result 3

$$\cdots+(-12520r^3-13112r^2+27736r-5360)yz^3+(1526r^3+2411r^2-658r+197)z^4=0.$$

Then heuristically there exists an isogeny of degree 2 between the Jacobians of X and Y, and both have CM by the maximal order $\mathbb{Z}_K$.

The sets $\mathcal{M}_{\mathbb{Z}_K}$ and $\mathcal{M}_{\mathbb{Z}_K}(\Phi)$.

We define by $\mathcal{M}_{\mathbb{Z}_K}$ = set of isomorphism classes of p.p.a. threefolds with primitive CM by $\mathbb{Z}_K$ modulo equivalence.
How do we efficiently compute representatives in $\mathcal{M}_{\mathbb{Z}_K}$?

Restrict to:

$$\mathcal{M}_{\mathbb{Z}_K}(\Phi) = \{(A, \Phi) : A \text{ is } p.p.a. \text{ threefold}, \ A = A(\Phi, \mathfrak{a}, \xi)\}.$$

$\rightsquigarrow$ $\mathcal{M}_{\mathbb{Z}_K}$ is disjoint union of $\mathcal{M}_{\mathbb{Z}_K}(\Phi)$ for all primitive CM type Φ modulo equivalence.

1. The Shimura class group $\mathcal{C}_K$ and its type norm subgroup.

Assume we have determined a triple $(\Phi, \mathfrak{a}, \xi) \in \mathcal{M}_{\mathbb{Z}_K}(\Phi)$.

The Shimura class group $\mathcal{C}_K$

$$\left\{(\mathfrak{b}, \beta) : \mathfrak{b} \text{ is fractional } \mathbb{Z}_K\text{-ideal}, \ \overline{\mathfrak{b}}\mathfrak{b} = \beta\mathbb{Z}_K, \ \beta \in K_0^* \text{ tot. pos.}\right\}$$

modulo equivalence.

Theorem

The action of the Shimura class group on the set $\mathcal{M}_{\mathbb{Z}_K}(\Phi)$ given by

$$\mathcal{C}_K \times \mathcal{M}_{\mathbb{Z}_K}(\Phi) \to \mathcal{M}_{\mathbb{Z}_K}(\Phi), \ ((\mathfrak{b}, \beta), (\Phi, \mathfrak{a}, \xi)) \mapsto (\Phi, \mathfrak{b}\mathfrak{a}, \beta^{-1}\xi)$$

is free and transitive.

2. The Shimura class group $\mathcal{C}_K$ and its type norm subgroup.

Using the fact that $\mathcal{M}_{\mathbb{Z}_K}(\Phi)$ is a $\mathcal{C}_K$-torsor we get:

Corollary

Any isogeny between p.p.a. threefolds with primitive CM by $\mathbb{Z}_K$ in $\mathcal{M}_{\mathbb{Z}_K}(\Phi)$ for a fixed Φ is induced by some $(\mathfrak{b}, \beta) \in \mathcal{C}_K$. □

3. The Shimura class group $\mathcal{C}_K$ and its type norm subgroup.

To compute $\mathcal{C}_K$ (isogenies in $\mathcal{M}_{\mathbb{Z}_K}(\Phi)$) requires an efficient computation of the group homomorphisms involved in the exact sequence

$$1 \to \frac{(\mathbb{Z}_{K_0}^*)^+}{N_{K/K_0}(\mathbb{Z}_K^*)} \xrightarrow{u \ \mapsto \ (\mathbb{Z}_K, u)} \mathcal{C}_K \xrightarrow{(\mathfrak{b}, \beta) \ \mapsto \ \mathfrak{b}} Cl(K) \xrightarrow{N_{K/K_0}} Cl(K_0^+) \to 1$$

4. The Shimura class group $\mathcal{C}_K$ and its type norm subgroup.

Is there a way to avoid an explicit computation of the Shimura group $\mathcal{C}_K$?

Theorem

Let K be a sextic CM field with Galois group isomorphic to C_6 or D_6. For any equivalence class $(\mathfrak{b}, \beta) \in \mathcal{C}_K$ the equivalence class of $(\mathfrak{b}^2, \beta')$ is in the image of the map

$$\mathcal{N} : Cl(K^r) \to \mathcal{C}_K, [\mathfrak{a}] \mapsto (N_{\Phi^r}(\mathfrak{a}), N(\mathfrak{a})),$$

where $\beta' = N(\mathfrak{b})^3$.

The theorem above allow us to proceed without any explicit computation of the reflex type norm N_{Φ^r}.

5. The Shimura class group $\mathcal{C}_K$ and its type norm subgroup.

Can we further restrict to hyperelliptic (non-hyperelliptic) CM points in $\mathcal{M}_{\mathbb{Z}_K}(\Phi)$?

Theorem

The set $\mathcal{M}_K(\Phi)$ is finite and stable under $G = \mathrm{Gal}(\overline{\mathbb{Q}}|K_0^r)$.

Corollary

There is a partition of $\mathcal{M}_{\mathbb{Z}_K}(\Phi)$ into G-orbits, where any G-orbit is induced by $(\mathcal{C}_K/\operatorname{im}\mathcal{N}) \times \mathcal{M}_K(\Phi) \to \mathcal{M}_K(\Phi)$.

- In the Corollary above we use the explicit Galois action in the First Main Theorem of CM.

5. The Shimura class group $\mathcal{C}_K$ and its type norm subgroup.

Can we further restrict to hyperelliptic (non-hyperelliptic) CM points in $\mathcal{M}_{\mathbb{Z}_K}(\Phi)$?

Theorem

The set $\mathcal{M}_K(\Phi)$ is finite and stable under $G = \mathrm{Gal}(\overline{\mathbb{Q}}|K_0^r)$.

Corollary

There is a partition of $\mathcal{M}_{\mathbb{Z}_K}(\Phi)$ into G-orbits, where any G-orbit is induced by $(\mathcal{C}_K/\operatorname{im}\mathcal{N}) \times \mathcal{M}_K(\Phi) \to \mathcal{M}_K(\Phi)$.

- In the Corollary above we use the explicit Galois action in the First Main Theorem of CM.
- Any G-orbit corresponds to Galois conjugate hyperelliptic, or non-hyperelliptic CM points in $\mathcal{M}_{\mathbb{Z}_K}(\Phi)$.

5. The Shimura class group $\mathcal{C}_K$ and its type norm subgroup.

Can we further restrict to hyperelliptic (non-hyperelliptic) CM points in $\mathcal{M}_{\mathbb{Z}_K}(\Phi)$?

Theorem

The set $\mathcal{M}_K(\Phi)$ is finite and stable under $G = \mathrm{Gal}(\overline{\mathbb{Q}}|K_0^r)$.

Corollary

There is a partition of $\mathcal{M}_{\mathbb{Z}_K}(\Phi)$ into G-orbits, where any G-orbit is induced by $(\mathcal{C}_K/\operatorname{im}\mathcal{N}) \times \mathcal{M}_K(\Phi) \to \mathcal{M}_K(\Phi)$.

- In the Corollary above we use the explicit Galois action in the First Main Theorem of CM.
- Any G-orbit corresponds to Galois conjugate hyperelliptic, or non-hyperelliptic CM points in $\mathcal{M}_{\mathbb{Z}_K}(\Phi)$.

The precomputation step.

Let K be a sextic CM field, and let K_0 be its totally real subfield.
Determine:

1. $\mathrm{Cl}(K), \mathbb{Z}_K^*$, $\mathrm{Cl}(K_0), \mathrm{Cl}^+(K_0)$, and $\mathbb{Z}_{K_0}^*$.
2. $G_1 = \{[\mathfrak{a}] \in \mathrm{Cl}(K) : \mathfrak{a}\bar{\mathfrak{a}} = \mu\mathbb{Z}_K \text{ for } \mu \in K_0\}$.
3. $G_2 = \{[\mathfrak{a}] \in G_1 : \mathfrak{a}\bar{\mathfrak{a}} = \mu\mathbb{Z}_K \text{ for } \mu \in K_0 \text{ totally positive}\}$.
4. Let $Q = G_2/eG_2$, where $e = 2$ if $\mathrm{Gal}(K) \in \{C_6, D_6\}$.
5. Set of ideals
    - $C = \{\mathfrak{c} \subset \mathbb{Z}_K : \mathfrak{c} \text{ is representative of } [\mathfrak{c}] \text{ in } G_1/G_2\}$, and
    - $B = \{\mathfrak{b} \subset \mathbb{Z}_K : \mathfrak{b} \text{ is representative of } [\mathfrak{b}] \text{ in } Q\}$.
6. $U_1 = \{u \in \mathbb{Z}_{K_0}^* : u \text{ is totally positive}\}$.
7. $U_2 = \{u \in U_1 : u \in \mathrm{im}\, N_{K/K_0}\}$.
8. Set of units
    - $W = \{w \in \mathbb{Z}_{K_0}^* : w \text{ is representative of } [w] \text{ in } \mathbb{Z}_{K_0}^*/U_1\}$, and
    - $V = \{v \in \mathbb{Z}_{K_0}^* : v \text{ is representative of } [v] \text{ in } U_1/U_2\}$.

The precomputation step.

Some explanations:

- We can compute the groups in step (1) by using class field methods in MAGMA.
- We can determine the subgroup
  - G_1 in Step (2) as the kernel of the homomorphism $\mathrm{Cl}(K) \to \mathrm{Cl}(K_0)$ given by $[\mathfrak{a}] \mapsto [\mathfrak{a}\overline{\mathfrak{a}}]$, and
  - G_2 as the kernel of a similar homomorphism to $\mathrm{Cl}^+(K_0)$.

The precomputation step.

Some explanations:

- We can compute the groups in step (1) by using class field methods in MAGMA.
- We can determine the subgroup
  - G_1 in Step (2) as the kernel of the homomorphism $\mathrm{Cl}(K) \to \mathrm{Cl}(K_0)$ given by $[\mathfrak{a}] \mapsto [\mathfrak{a}\bar{\mathfrak{a}}]$, and
  - G_2 as the kernel of a similar homomorphism to $\mathrm{Cl}^+(K_0)$.
  - Similar considerations apply to the determination of U_1 and U_2 in Steps (6) and (7).

The precomputation step.

Some explanations:

- We can compute the groups in step (1) by using class field methods in MAGMA.
- We can determine the subgroup
  - G_1 in Step (2) as the kernel of the homomorphism $\mathrm{Cl}(K) \to \mathrm{Cl}(K_0)$ given by $[\mathfrak{a}] \mapsto [\mathfrak{a}\overline{\mathfrak{a}}]$, and
  - G_2 as the kernel of a similar homomorphism to $\mathrm{Cl}^+(K_0)$.
  - Similar considerations apply to the determination of U_1 and U_2 in Steps (6) and (7).
  - The remaining points imply more technical details which we explain in our paper.

The precomputation step.

Some explanations:

- We can compute the groups in step (1) by using class field methods in MAGMA.
- We can determine the subgroup
  - G_1 in Step (2) as the kernel of the homomorphism $\mathrm{Cl}(K) \to \mathrm{Cl}(K_0)$ given by $[\mathfrak{a}] \mapsto [\mathfrak{a}\overline{\mathfrak{a}}]$, and
  - G_2 as the kernel of a similar homomorphism to $\mathrm{Cl}^+(K_0)$.
  - Similar considerations apply to the determination of U_1 and U_2 in Steps (6) and (7).
  - The remaining points imply more technical details which we explain in our paper.

Algorithms.

We use the objects computed in the precomputation step in the following algorithms:

1. Algorithm that determines an initial triple $(\Phi, \mathfrak{a}, \xi)$.
2. Algorithm that uses (1) to determine all triples $(\Phi, \mathfrak{a}, \xi)$.
3. Algorithm that calculates period matrices of all p.p.a.v. found using (2) and automatically sorts them into sets of hyperelliptic and non-hyperelliptic Jacobains.

We used these algorithms to find our main results.

Our code is implemented in MAGMA [BCP97] and available at [DIS21].

Thank you for listening!

Wieb Bosma, John Cannon, and Catherine Playoust.
The Magma algebra system. I. The user language.
J. Symbolic Comput., 24(3-4):235–265, 1997.
Computational algebra and number theory (London, 1993).

Jennifer S. Balakrishnan, Sorina Ionica, Kristin Lauter, and Christelle Vincent.
Constructing genus-3 hyperelliptic Jacobians with CM.
LMS J. Comput. Math., 19(suppl. A):283–300, 2016.

Claus Diem.
An index calculus algorithm for plane curves of small degree.
In Florian Hess, Sebastian Pauli, and Michael E. Pohst, editors, *Algorithmic Number Theory, 7th International Symposium, ANTS-VII, Berlin, Germany, July 23-28, 2006, Proceedings*, volume 4076 of *Lecture Notes in Computer Science*, pages 543–557. Springer, 2006.

Bogdan Dina, Sorina Ionica, and Jeroen Sijsling.

cm-calculations, a Magma package for calculating with CM curves.

https://github.com/JRSijsling/cm-calculations, 2021.

Pierrick Gaudry, Emmanuel Thomé, Nicolas Thériault, and Claus Diem.
A double large prime variation for small genus hyperelliptic index calculus.
Math. Comput., 76(257):475–492, 2007.

Bruno Klingler and Andrei Yafaev.
The André-Oort conjecture.
Annals of Mathematics, 180:867–925, 2014.

Pınar Kılıçer.
The CM class number one problem for curves.
PhD thesis, Universiteit Leiden, 2016.

MarcoMarco Streng.
Complex multiplication of abelian surfaces.

PhD thesis, Universiteit Leiden, 2010.

Annegret Weng.
A class of hyperelliptic CM-curves of genus three.
J. Ramanujan Math. Soc., 16(4):339–372, 2001.