Principally polarized squares of elliptic curves with field of moduli equal to $\mathbb{Q}$

Alexandre Gélin Everett W. Howe Christophe Ritzenthaler

Laboratoire de Mathématiques de Versailles, France
CCR San Diego, USA Université de Rennes 1, France

ANTS XIII - Madison

2018/07/16

Principally polarized squares of elliptic curves with field of moduli equal to $\mathbb{Q}$

Alexandre Gélin   Everett W. Howe   Christophe Ritzenthaler

Laboratoire de Mathématiques de Versailles, France
CCR San Diego, USA   Université de Rennes 1, France

ANTS XIII - Madison

2018/07/16

Our result

Proposition

- There exist exactly 46 genus-2 curves over $\overline{\mathbb{Q}}$ with field of moduli $\mathbb{Q}$ whose Jacobians are isomorphic to the square of an elliptic curve with complex multiplication by a maximal order.
- Among these 46 curves exactly 13 can be defined over $\mathbb{Q}$.

Problem statement

- Genus-2 curves $\longrightarrow$ Princ. polarized abelian varieties of dim. 2

Problem statement

- Genus-2 curves $\longrightarrow$ Princ. polarized abelian varieties of dim. 2
- Field of moduli: the field fixed by $\{\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \mid A \simeq A^\sigma\}$

Problem statement

- Genus-2 curves $\longrightarrow$ Princ. polarized abelian varieties of dim. 2
- Field of moduli $\mathbb{Q} \longleftrightarrow$ Rational points in the moduli space

Problem statement

- Genus-2 curves $\longrightarrow$ Princ. polarized abelian varieties of dim. 2
- Field of moduli $\mathbb{Q}$ $\longleftrightarrow$ Rational points in the moduli space
- CM: endomorphism ring contains an order in a number field

Problem statement

- Genus-2 curves $\longrightarrow$ Princ. polarized abelian varieties of dim. 2
- Field of moduli $\mathbb{Q} \longleftrightarrow$ Rational points in the moduli space
- CM: endomorphism ring contains an order in a number field
- Simple case: well-known in genus 1, 2 and 3

Problem statement

- Genus-2 curves $\longrightarrow$ Princ. polarized abelian varieties of dim. 2
- Field of moduli $\mathbb{Q} \longleftrightarrow$ Rational points in the moduli space
- CM: endomorphism ring contains an order in a number field
- Simple case: well-known in genus 1, 2 and 3
- Non-simple case: $A \sim E^2 \Longleftrightarrow A \simeq E_1 \times E_2$

Problem statement

- Genus-2 curves $\longrightarrow$ Princ. polarized abelian varieties of dim. 2
- Field of moduli $\mathbb{Q} \longleftrightarrow$ Rational points in the moduli space
- CM: endomorphism ring contains an order in a number field
- Simple case: well-known in genus 1, 2 and 3
- Non-simple case: $A \sim E^2 \Longleftrightarrow A \simeq E_1 \times E_2$
- Additional constraint: we focus on $A \simeq E^2$

Problem statement

- Genus-2 curves $\longrightarrow$ Princ. polarized abelian varieties of dim. 2
- Field of moduli $\mathbb{Q} \longleftrightarrow$ Rational points in the moduli space
- CM: endomorphism ring contains an order in a number field
- Simple case: well-known in genus 1, 2 and 3
- Non-simple case: $A \sim E^2 \Longleftrightarrow A \simeq E_1 \times E_2$
- Additional constraint: we focus on $A \simeq E^2$
- E must be a CM elliptic curve

Problem statement

- Genus-2 curves $\longrightarrow$ Princ. polarized abelian varieties of dim. 2
- Field of moduli $\mathbb{Q} \longleftrightarrow$ Rational points in the moduli space
- CM: endomorphism ring contains an order in a number field
- Simple case: well-known in genus 1, 2 and 3
- Non-simple case: $A \sim E^2 \Longleftrightarrow A \simeq E_1 \times E_2$
- Additional constraint: we focus on $A \simeq E^2$
- E must be a CM elliptic curve
- For simplicity, we only consider E with CM by a maximal order

Conditions on E^2

$\mathbb{Q}$ is field of moduli $\implies$ $(E^2, \varphi) \simeq (E^2, \varphi)^\sigma$ for all $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$

Conditions on E^2

$\mathbb{Q}$ is field of moduli $\implies$ $(E^2, \varphi) \simeq (E^2, \varphi)^\sigma$ for all $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$

$\implies$ $E^2 \simeq (E^\sigma)^2$ for all $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{K})$
(with $\mathbb{K}$ the CM-field for E)

Conditions on E^2

$\mathbb{Q}$ is field of moduli	$\Longrightarrow$	$(E^2,\varphi) \simeq (E^2,\varphi)^\sigma$	for all $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$
	$\Longrightarrow$	$E^2 \simeq (E^\sigma)^2$	for all $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{K})$ (with $\mathbb{K}$ the CM-field for E)
CM-theory	$\Longrightarrow$	$E^\sigma \simeq E/I_\sigma$	for $I_\sigma \in \mathrm{Cl}(\mathscr{O})$

Conditions on E^2

$\mathbb{Q}$ is field of moduli	$\Longrightarrow$	$(E^2, \varphi) \simeq (E^2, \varphi)^\sigma$	for all $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$
	$\Longrightarrow$	$E^2 \simeq (E^\sigma)^2$	for all $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{K})$ (with $\mathbb{K}$ the CM-field for E)
CM-theory	$\Longrightarrow$	$E^\sigma \simeq E/I_\sigma$	for $I_\sigma \in \mathrm{Cl}(\mathscr{O})$
Kani (2011)	$\Longrightarrow$	$E^2 \simeq (E/I_\sigma)^2$	$\Longleftrightarrow$ $I_\sigma^2 = [\mathscr{O}]$

Conditions on E^2

$\mathbb{Q}$ is field of moduli	$\Longrightarrow$	$(E^2,\varphi) \simeq (E^2,\varphi)^\sigma$	for all $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$
	$\Longrightarrow$	$E^2 \simeq (E^\sigma)^2$	for all $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{K})$ (with $\mathbb{K}$ the CM-field for E)
CM-theory	$\Longrightarrow$	$E^\sigma \simeq E/I_\sigma$	for $I_\sigma \in \mathrm{Cl}(\mathcal{O})$
Kani (2011)	$\Longrightarrow$	$E^2 \simeq (E/I_\sigma)^2$	$\Longleftrightarrow$ $I_\sigma^2 = [\mathcal{O}]$

Proposition

A necessary condition for the field of moduli $\mathbf{M}$ to be contained in $\mathbb{K}$ is that the class group of $\mathcal{O}$ has exponent at most 2.

Conditions on E^2

$\mathbb{Q}$ is field of moduli	$\Longrightarrow$	$(E^2, \varphi) \simeq (E^2, \varphi)^\sigma$	for all $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$
	$\Longrightarrow$	$E^2 \simeq (E^\sigma)^2$	for all $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{K})$ (with $\mathbb{K}$ the CM-field for E)
CM-theory	$\Longrightarrow$	$E^\sigma \simeq E/I_\sigma$	for $I_\sigma \in \mathrm{Cl}(\mathcal{O})$
Kani (2011)	$\Longrightarrow$	$E^2 \simeq (E/I_\sigma)^2$	$\Longleftrightarrow$ $I_\sigma^2 = [\mathcal{O}]$

Proposition

A necessary condition for the field of moduli $\mathbf{M}$ to be contained in $\mathbb{K}$ is that the class group of $\mathcal{O}$ has exponent at most 2.

Fact

Assuming the Generalized Riemann Hypothesis, there exist 65 fundamental discriminants whose class group is of exponent at most 2.

Conditions on E^2

$\#\mathrm{Cl}(\mathcal{O})$	Discriminants Δ
2^0	$-3, -4, -7, -8, -11, -19, -43, -67, -163$
2^1	$-15, -20, -24, -35, -40, -51, -52, -88, -91, -115, -123, -148, -187, -232, -235, -267, -403, -427$
2^2	$-84, -120, -132, -168, -195, -228, -280, -312, -340, -372, -408, -435, -483, -520, -532, -555, -595, -627, -708, -715, -760, -795, -1012, -1435$
2^3	$-420, -660, -840, -1092, -1155, -1320, -1380, -1428, -1540, -1848, -1995, -3003, -3315$
2^4	-5460

Polarizations over E^2

- Principal polarization $\longrightarrow$ isogeny of degree 1 from E^2 to $\widehat{E^2}$

Polarizations over E^2

- Principal polarization $\longrightarrow$ isogeny of degree 1 from E^2 to $\widehat{E^2}$
- One particular example: the product polarization $\varphi_0 = \varphi_E \times \varphi_E$

Polarizations over E^2

- Principal polarization $\longrightarrow$ isogeny of degree 1 from E^2 to $\widehat{E^2}$
- One particular example: the product polarization $\varphi_0 = \varphi_E \times \varphi_E$
- Characterization: $\varphi = \varphi_0 \cdot M$ for M positive definite unimodular Hermitian matrices with coefficients in $\mathcal{O}$

Polarizations over E^2

- Principal polarization $\longrightarrow$ isogeny of degree 1 from E^2 to $\widehat{E^2}$
- One particular example: the product polarization $\varphi_0 = \varphi_E \times \varphi_E$
- Characterization: $\varphi = \varphi_0 \cdot M$ for M positive definite unimodular Hermitian matrices with coefficients in $\mathcal{O}$
- Isomorphic polarizations $\longleftrightarrow$ Congruent matrices

Polarizations over E^2

- Principal polarization $\longrightarrow$ isogeny of degree 1 from E^2 to $\widehat{E^2}$
- One particular example: the product polarization $\varphi_0 = \varphi_E \times \varphi_E$
- Characterization: $\varphi = \varphi_0 \cdot M$ for M positive definite unimodular Hermitian matrices with coefficients in $\mathscr{O}$
- Isomorphic polarizations $\longleftrightarrow$ Congruent matrices

Proposition

In genus 2, (E^2, φ) is a Jacobian $\iff$ φ is not decomposable $\iff$ M is not congruent to a diagonal matrix.

Find the polarizations

- One representative per isomorphism class
  $\longrightarrow$ a matrix M with small coefficients

Find the polarizations

- One representative per isomorphism class
  $\longrightarrow$ a matrix M with small coefficients
- We know the number of polarizations for each order
  Hayashida (1968)

Find the polarizations

- One representative per isomorphism class

  $\longrightarrow$ a matrix M with small coefficients

- We know the number of polarizations for each order

  Hayashida (1968)

- Enumerate all matrices $\begin{pmatrix} a & b \\ \bar{b} & P/a \end{pmatrix}$ for P increasing in $\mathbb{N}$, a dividing P and $\mathrm{Norm}(b) = P - 1$

Find the polarizations

- One representative per isomorphism class

  $\longrightarrow$ a matrix M with small coefficients

- We know the number of polarizations for each order

  Hayashida (1968)

- Enumerate all matrices $\begin{pmatrix} a & b \\ \bar{b} & P/a \end{pmatrix}$ for P increasing in $\mathbb{N}$, a dividing P and $\mathrm{Norm}(b) = P - 1$

Fact

For the 65 possible orders, there exist 1226 indecomposable principal polarizations.

Conditions on (E^2, φ)

- $\mathbf{M} \subseteq \mathbb{K}$ is field of moduli $\iff \forall \sigma \in \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{K}\right)$, $\left(E^2, \varphi\right) \simeq \left(E^2, \varphi\right)^{\sigma}$, *i.e.*, the following diagram commutes

$$
\begin{array}{ccccc}
E^2 & \xrightarrow{\;M\;} & E^2 & \xrightarrow{\;\varphi_0\;} & \widehat{E^2} \\
\Big\downarrow{\scriptstyle \alpha_\sigma} & & & & \Big\uparrow{\scriptstyle \widehat{\alpha}_\sigma} \\
\left(E^\sigma\right)^2 & \xrightarrow{\;M\;} & \left(E^\sigma\right)^2 & \xrightarrow{\;\varphi_0^\sigma\;} & \left(\widehat{E^\sigma}\right)^2
\end{array}
$$

Conditions on $\left(E^2, \varphi\right)$

- $\mathbf{M} \subseteq \mathbb{K}$ is field of moduli $\iff \forall \sigma \in \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{K}\right)$, $\left(E^2, \varphi\right) \simeq \left(E^2, \varphi\right)^\sigma$, *i.e.*, the following diagram commutes

$$\begin{array}{ccccc}
E^2 & \xrightarrow{\quad M \quad} & E^2 & \xrightarrow{\quad \varphi_0 \quad} & \widehat{E^2} \\
\Big\downarrow{\scriptstyle \alpha_\sigma} & & & & \Big\uparrow{\scriptstyle \widehat{\alpha}_\sigma} \\
\left(E^\sigma\right)^2 & \xrightarrow{\quad M \quad} & \left(E^\sigma\right)^2 & \xrightarrow{\quad \varphi_0^\sigma \quad} & \left(\widehat{E^\sigma}\right)^2
\end{array}$$

- In terms of ideals, if $E^\sigma \simeq E/I_\sigma$ with $I_\sigma \in \mathrm{Cl}(\mathscr{O})$ and $\mathfrak{a}_\sigma \in I_\sigma$, then $\forall \sigma \in \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{K}\right)$, $\exists P \in \mathrm{GL}_2(\mathfrak{a}_\sigma)$ such that $\left(n = \mathrm{Norm}(\mathfrak{a}_\sigma)\right)$

$$nM = P^* M P$$

Enumeration process

- Suppose there exists a matrix P such that $nM = P^* MP$.

Enumeration process

- Suppose there exists a matrix P such that $nM = P^* MP$.
- If $M = \begin{pmatrix} a & b \\ \bar{b} & d \end{pmatrix}$, let us take $L = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$, so that $L^* L = aM$.

Enumeration process

- Suppose there exists a matrix P such that $nM = P^* MP$.
- If $M = \begin{pmatrix} a & b \\ \bar{b} & d \end{pmatrix}$, let us take $L = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$, so that $L^* L = aM$.
- Let $Q = LPL^{-1}$. Then $nM = P^* MP$ becomes $n\mathrm{Id} = Q^* Q$.

Enumeration process

- Suppose there exists a matrix P such that $nM = P^* MP$.
- If $M = \begin{pmatrix} a & b \\ \bar{b} & d \end{pmatrix}$, let us take $L = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$, so that $L^* L = aM$.
- Let $Q = LPL^{-1}$. Then $nM = P^* MP$ becomes $n\mathrm{Id} = Q^* Q$.
- Hence Q must be of the form $\begin{pmatrix} x & y \\ z & t \end{pmatrix}$ with x, y, z, $t \in \mathbb{K}$ satisfying

  $\mathrm{Norm}(x) + \mathrm{Norm}(z) = \mathrm{Norm}(y) + \mathrm{Norm}(t) = n$ and $\bar{x}y + \bar{z}t = 0.$

Enumeration process

- Suppose there exists a matrix P such that $nM = P^* MP$.
- If $M = \left(\begin{smallmatrix} a & b \\ \bar{b} & d \end{smallmatrix}\right)$, let us take $L = \left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right)$, so that $L^* L = aM$.
- Let $Q = LPL^{-1}$. Then $nM = P^* MP$ becomes $n\mathrm{Id} = Q^* Q$.
- Hence Q must be of the form $\left(\begin{smallmatrix} x & y \\ z & t \end{smallmatrix}\right)$ with x, y, z, $t \in \mathbb{K}$ satisfying

  $\mathrm{Norm}(x) + \mathrm{Norm}(z) = \mathrm{Norm}(y) + \mathrm{Norm}(t) = n$ and $\bar{x}y + \bar{z}t = 0$.
- And

$$P = L^{-1} QL = \begin{pmatrix} x - bz & \frac{bx+y-b^2z-bt}{a} \\ az & bz + t \end{pmatrix} \in M_2(\mathfrak{a}_\sigma).$$

Enumeration process

- For every polarization

  For every ideal class $I_\sigma \in \mathrm{Cl}(\mathcal{O})$

    Compute the solutions of the norm equation

    Check whether the matrix P lies in $M_2(\mathfrak{a}_\sigma)$

Enumeration process

- For every polarization

  For every ideal class $I_\sigma \in \mathrm{Cl}(\mathcal{O})$

  Compute the solutions of the norm equation

  Check whether the matrix P lies in $M_2(\mathfrak{a}_\sigma)$

- If we have a matrix P for each class, then $\mathbf{M} \subseteq \mathbb{K}$

Enumeration process

- For every polarization

  For every ideal class $I_\sigma \in \mathrm{Cl}(\mathscr{O})$

  Compute the solutions of the norm equation

  Check whether the matrix P lies in $M_2(\mathfrak{a}_\sigma)$

- If we have a matrix P for each class, then $\mathbf{M} \subseteq \mathbb{K}$

- Eventually, we get $\mathbf{M} = \mathbb{Q}$ as $\mathbb{Q}\big(j(E)\big)$ is totally real

Enumeration process

- For every polarization

  For every ideal class $I_\sigma \in \mathrm{Cl}(\mathcal{O})$

  Compute the solutions of the norm equation

  Check whether the matrix P lies in $M_2(\mathfrak{a}_\sigma)$

- If we have a matrix P for each class, then $\mathbf{M} \subseteq \mathbb{K}$

- Eventually, we get $\mathbf{M} = \mathbb{Q}$ as $\mathbb{Q}\big(j(E)\big)$ is totally real

Fact

Among the 1226 Jacobians of genus-2 curves identified earlier, 46 have their field of moduli equal to $\mathbb{Q}$.

Construction of the invariants

- Polarization $\longrightarrow$ Matrix M $\longrightarrow$ Riemann matrix

- Polarization $\longrightarrow$ Matrix M $\longrightarrow$ Riemann matrix
- Compute the *theta* constants

Construction of the invariants

- Polarization $\longrightarrow$ Matrix M $\longrightarrow$ Riemann matrix

- Compute the *theta* constants

- With $\lambda_1 = \frac{\theta_0^2\theta_2^2}{\theta_1^2\theta_3^2}$, $\lambda_2 = \frac{\theta_2^2\theta_7^2}{\theta_3^2\theta_9^2}$, and $\lambda_3 = \frac{\theta_0^2\theta_7^2}{\theta_1^2\theta_9^2}$, we get the model

$$C : y^2 = x(x-1)(x-\lambda_1)(x-\lambda_2)(x-\lambda_3)$$

Construction of the invariants

- Polarization $\longrightarrow$ Matrix M $\longrightarrow$ Riemann matrix
- Compute the *theta* constants
- With $\lambda_1 = \frac{\theta_0^2\theta_2^2}{\theta_1^2\theta_3^2}$, $\lambda_2 = \frac{\theta_2^2\theta_7^2}{\theta_3^2\theta_9^2}$, and $\lambda_3 = \frac{\theta_0^2\theta_7^2}{\theta_1^2\theta_9^2}$, we get the model

$$C : y^2 = x(x-1)(x-\lambda_1)(x-\lambda_2)(x-\lambda_3)$$

- Compute an approximation of the Cardona-Quer invariants

Construction of the invariants

- Polarization $\longrightarrow$ Matrix M $\longrightarrow$ Riemann matrix
- Compute the *theta* constants
- With $\lambda_1 = \frac{\theta_0^2\theta_2^2}{\theta_1^2\theta_3^2}$, $\lambda_2 = \frac{\theta_2^2\theta_7^2}{\theta_3^2\theta_9^2}$, and $\lambda_3 = \frac{\theta_0^2\theta_7^2}{\theta_1^2\theta_9^2}$, we get the model

$$C : y^2 = x(x-1)(x-\lambda_1)(x-\lambda_2)(x-\lambda_3)$$

- Compute an approximation of the Cardona-Quer invariants
- Recognize them as rationals (special form for denominators)

Models over $\mathbb{Q}$

- If $|\mathrm{Aut}(C)| > 2$, the field of moduli is a field of definition [CQ05]

Models over $\mathbb{Q}$

- If $|\mathrm{Aut}(C)| > 2$, the field of moduli is a field of definition [CQ05]
- If $|\mathrm{Aut}(C)| = 2$, not even a model over $\mathbb{R}$

Models over $\mathbb{Q}$

- If $|\mathrm{Aut}(C)| > 2$, the field of moduli is a field of definition [CQ05]
- If $|\mathrm{Aut}(C)| = 2$, not even a model over $\mathbb{R}$
- Easy to compute the group of automorphisms of (E^2, φ) (matrices P such that $P^* M P = M$)

Models over $\mathbb{Q}$

- If $|\mathrm{Aut}(C)| > 2$, the field of moduli is a field of definition [CQ05]
- If $|\mathrm{Aut}(C)| = 2$, not even a model over $\mathbb{R}$
- Easy to compute the group of automorphisms of (E^2, φ) (matrices P such that $P^* MP = M$)

Fact

Among the 46 genus-2 curves with field of moduli $\mathbb{Q}$, 13 have a model over $\mathbb{Q}$.

Models over $\mathbb{Q}$

- If $|\mathrm{Aut}(C)| > 2$, the field of moduli is a field of definition [CQ05]
- If $|\mathrm{Aut}(C)| = 2$, not even a model over $\mathbb{R}$
- Easy to compute the group of automorphisms of (E^2, φ)
(matrices P such that $P^* M P = M$)

Fact

Among the 46 genus-2 curves with field of moduli $\mathbb{Q}$, 13 have a model over $\mathbb{Q}$.

Proof

For these 13 curves, we have proven that the invariants are correct by having computed the endomorphism ring.

Costa-Mascot-Sijsling-Voight (2017)

Thanks

Thank you