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 $\mathbb{Q}$. 
Genus-2 curves $\rightarrow$ Principally polarized abelian varieties of dim. 2
Problem statement

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

- Field of moduli: the field fixed by $\{\sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \mid A \cong A^\sigma\}$
Problem statement

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

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

- Genus-2 curves $\rightarrow$ Princ. polarized abelian varieties of dim. 2
- Field of moduli $\mathbb{Q} \leftrightarrow$ 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 $\rightarrow$ Princ. polarized abelian varieties of dim. 2
- Field of moduli $\mathbb{Q} \leftrightarrow$ 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: $A \sim E^2 \iff A \cong E_1 \times E_2$

Alexandre Gélin
Principally polarized squares of elliptic curves
Problem statement

- Genus-2 curves $\rightarrow$ Princ. polarized abelian varieties of dim. 2
- Field of moduli $\mathbb{Q} \leftrightarrow$ 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: $A \sim E^2 \iff A \cong E_1 \times E_2$
- Additional constraint: we focus on $A \cong E^2$
Problem statement

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

- Field of moduli $\mathbb{Q} \leftrightarrow$ 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: $A \sim E^2 \iff A \cong E_1 \times E_2$

- Additional constraint: we focus on $A \cong E^2$

- $E$ must be a CM elliptic curve
Problem statement

- Genus-2 curves $\rightarrow$ Princ. polarized abelian varieties of dim. 2
- Field of moduli $\mathbb{Q} \leftrightarrow$ 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: $A \sim E^2 \iff A \cong E_1 \times E_2$
- Additional constraint: we focus on $A \cong E^2$
- $E$ 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 $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$
Conditions on $E^2$

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

\( \implies E^2 \approx (E^\sigma)^2 \) for all \( \sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{K}) \)

(with \( \mathbb{K} \) the CM-field for \( E \))
 Conditions on $E^2$

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

$\implies E^2 \simeq (E^\sigma)^2$ for all $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{K})$

(with $\mathbb{K}$ the CM-field for $E$)

CM-theory $\implies E^\sigma \simeq E/I_\sigma$ for $I_\sigma \in \text{Cl}(\mathcal{O})$

---

Principally polarized squares of elliptic curves

---

Alexandre Gélin
Conditions on $E^2$

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

$\implies E^2 \simeq (E^\sigma)^2$ for all $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{K})$

(with $\mathbb{K}$ the CM-field for $E$)

CM-theory $\implies E^\sigma \simeq E/I_\sigma$ for $I_\sigma \in \text{Cl}(\mathcal{O})$

Kani (2011) $\implies E^2 \simeq (E/I_\sigma)^2$ $\iff I_\sigma^2 = [\mathcal{O}]$
Conditions on $E^2$

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

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

CM-theory $\implies E^\sigma \simeq E/I_\sigma$ for $I_\sigma \in \text{Cl}(\mathcal{O})$

- Kani (2011) $\implies E^2 \simeq (E/I_\sigma)^2$ $\iff I_\sigma^2 = [\mathcal{O}]$

Proposition

A necessary condition for the field of moduli $\mathcal{M}$ 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 $\implies (E^2, \varphi) \simeq (E^2, \varphi)^\sigma$ for all $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$

$\implies E^2 \simeq (E^\sigma)^2$ for all $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{K})$

(with $\mathbb{K}$ the CM-field for $E$)

CM-theory $\implies E^\sigma \simeq E/I_\sigma$ for $I_\sigma \in \text{Cl}(\mathcal{O})$

Kani (2011) $\implies E^2 \simeq (E/I_\sigma)^2 \iff I_{\sigma}^2 = [\mathcal{O}]$

**Proposition**

A necessary condition for the field of moduli $\mathcal{M}$ 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 $E^2$

<table>
<thead>
<tr>
<th>$#\text{Cl}(O)$</th>
<th>Discriminants $\Delta$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$2^0$</td>
<td>$-3, -4, -7, -8, -11, -19, -43, -67, -163$</td>
</tr>
<tr>
<td>$2^3$</td>
<td>$-420, -660, -840, -1092, -1155, -1320, -1380, -1428, -1540, -1848, -1995, -3003, -3315$</td>
</tr>
<tr>
<td>$2^4$</td>
<td>$-5460$</td>
</tr>
</tbody>
</table>

Alexandre Gélin

Principally polarized squares of elliptic curves
Polarizations over $E^2$

- Principal polarization $\mapsto$ isogeny of degree 1 from $E^2$ to $\hat{E}^2$
Polarizations over $E^2$

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

- 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 $\hat{E}^2$
- 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 $\hat{E}^2$
- 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 $\rightarrow$ isogeny of degree 1 from $E^2$ to $\hat{E}^2$
- 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 $\leftrightarrow$ Congruent matrices

**Proposition**

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

- One representative per isomorphism class
  \[ \rightarrow \text{a matrix } M \text{ with small coefficients} \]
Find the polarizations

- One representative per isomorphism class
  \( \rightarrow \) 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 → 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 $\text{Norm}(b) = P - 1$
One representative per isomorphism class

\[ \rightarrow \text{a matrix } M \text{ with small coefficients} \]

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 \( \text{Norm}(b) = P - 1 \)

Fact

For the 65 possible orders, there exist 1226 indecomposable principal polarizations.
Conditions on \((E^2, \varphi)\)

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

\[
\begin{array}{cccccc}
E^2 & \xrightarrow{M} & E^2 & \xrightarrow{\varphi_0} & \hat{E}^2 \\
\alpha_{\sigma} & & & & & \hat{\alpha}_{\sigma} \\
(E^\sigma)^2 & \xrightarrow{M} & (E^\sigma)^2 & \xrightarrow{\varphi_0^\sigma} & (\hat{E}^\sigma)^2
\end{array}
\]
Conditions on $(E^2, \varphi)$

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

\[
\begin{array}{ccc}
E^2 & \xrightarrow{M} & E^2 \\
\downarrow{\alpha_\sigma} & & \downarrow{\varphi_0}
\end{array}
\begin{array}{ccc}
(E^\sigma)^2 & \xrightarrow{M} & (E^\sigma)^2 \\
\downarrow{\alpha_\sigma} & & \downarrow{\varphi_0^\sigma}
\end{array}
\begin{array}{ccc}
\hat{E}^2 & \xrightarrow{\hat{\alpha}_\sigma} & \hat{E}^2 \\
\end{array}
\]

- In terms of ideals, if $E^\sigma \cong E/I_\sigma$ with $I_\sigma \in \text{Cl}(\mathcal{O})$ and $a_\sigma \in I_\sigma$, then $\forall \sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{K})$, $\exists P \in \text{GL}_2(a_\sigma)$ such that ($n = \text{Norm}(a_\sigma)$)

\[nM = P^* MP\]
Suppose there exists a matrix $P$ such that $nM = P^* MP$. 
Suppose there exists a matrix $P$ such that $nM = P^*MP$.

If $M = \begin{pmatrix} a & b \\ b & d \end{pmatrix}$, let us take $L = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$, so that $L^*L = aM$. 

Hence $Q = LPL^{-1}$. Then $nM = P^*MP$ becomes $nI = Q^*Q$.

And $P = L^{-1}QL = \begin{pmatrix} x & y \\ z & t \end{pmatrix}$ with $x, y, z, t \in \mathbb{K}$ satisfying $\text{Norm}(x) + \text{Norm}(z) = \text{Norm}(y) + \text{Norm}(t) = n$ and $\bar{xy} + \bar{zt} = 0$. 

And $P = L^{-1}QL = \begin{pmatrix} x - bz \\ bx + y - b^2z - bt \\ a \end{pmatrix} \in M_2(\mathbb{K})$. 

Alexandre Gélin

Principally polarized squares of elliptic curves
Suppose there exists a matrix $P$ such that $nM = P^* MP$.

If $M = \begin{pmatrix} a & b \\ b & d \end{pmatrix}$, 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 $n\text{Id} = Q^* Q$. 
Suppose there exists a matrix $P$ such that $nM = P^*MP$.

If $M = \begin{pmatrix} a & b \\ b & d \end{pmatrix}$, 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 $n\text{Id} = Q^*Q$.

Hence $Q$ must be of the form $\begin{pmatrix} x & y \\ z & t \end{pmatrix}$ with $x, y, z, t \in \mathbb{K}$ satisfying

$$\text{Norm}(x) + \text{Norm}(z) = \text{Norm}(y) + \text{Norm}(t) = n \quad \text{and} \quad \bar{x}y + \bar{z}t = 0.$$
Suppose there exists a matrix $P$ such that $nM = P^* MP$.

If $M = \begin{pmatrix} a & b \\ b & d \end{pmatrix}$, 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 $n\text{Id} = Q^* Q$.

Hence $Q$ must be of the form $\begin{pmatrix} x & y \\ z & t \end{pmatrix}$ with $x, y, z, t \in \mathbb{K}$ satisfying

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

And

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

- For every polarization
  - For every ideal class $I_\sigma \in \text{Cl}(\mathcal{O})$
    - Compute the solutions of the norm equation
    - Check whether the matrix $P$ lies in $M_2(\mathbb{a}_\sigma)$
Enumeration process

- For every polarization
  - For every ideal class $I_\sigma \in \text{Cl}(\mathcal{O})$
    - Compute the solutions of the norm equation
    - Check whether the matrix $P$ lies in $M_2(\alpha_\sigma)$
- If we have a matrix $P$ for each class, then $\mathbf{M} \subseteq \mathbf{K}$
Enumeration process

- For every polarization
  - For every ideal class $I_\sigma \in \text{Cl}(\mathcal{O})$
    - Compute the solutions of the norm equation
    - Check whether the matrix $P$ lies in $M_2(\alpha_\sigma)$
  
- If we have a matrix $P$ for each class, then $M \subseteq K$

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

Fact

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

Alexandre Gélin

Principally polarized squares of elliptic curves
Enumeration process

- For every polarization
  - For every ideal class $I_\sigma \in \text{Cl}(\mathcal{O})$
    - Compute the solutions of the norm equation
    - Check whether the matrix $P$ lies in $M_2(a_\sigma)$

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

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

Fact

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

Alexandre Gélin: Principally polarized squares of elliptic curves
Construction of the invariants

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

Compute the $\theta$ constants with

\[
\begin{align*}
\lambda_1 &= \theta_2^0 \theta_2^1 \theta_2^3, \\
\lambda_2 &= \theta_2^2 \theta_2^7 \theta_2^9, \\
\lambda_3 &= \theta_2^0 \theta_2^7 \theta_2^1 \theta_2^9,
\end{align*}
\]

we get the model

\[
y_2 = x(x - 1)(x - \lambda_1)(x - \lambda_2)(x - \lambda_3)
\]

Compute an approximation of the Cardona-Quer invariants

Recognize them as rationals (special form for denominators)
Construction of the invariants

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

- Compute the $\theta$ constants

- $\lambda_1 = \theta_2^{10}\theta_2^{20}\theta_2^{30}$, $\lambda_2 = \theta_2^{20}\theta_2^{70}\theta_2^{90}$, and $\lambda_3 = \theta_2^{100}\theta_2^{70}\theta_2^{100}\theta_2^{90}$, 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)
Construction of the invariants

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

- Compute the theta constants

- With $\lambda_1 = \frac{\theta_2^2 \theta_7^2}{\theta_1^2 \theta_3^2}$, $\lambda_2 = \frac{\theta_2^2 \theta_7^2}{\theta_3^2 \theta_9^2}$, 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 $\rightarrow$ Matrix $M$ $\rightarrow$ Riemann matrix

- Compute the \textit{theta} constants

- With $\lambda_1 = \frac{\theta_2^2\theta_4^2}{\theta_1^2\theta_3^2}$, $\lambda_2 = \frac{\theta_2^2\theta_7^2}{\theta_3^2\theta_9^2}$, 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 $\rightarrow$ Matrix $M$ $\rightarrow$ 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)
If $|\text{Aut}(C)| > 2$, the field of moduli is a field of definition \[\text{CQ05}\]
Models over $\mathbb{Q}$

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

- If $|\text{Aut}(C)| = 2$, not even a model over $\mathbb{R}$

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)
If |Aut(C)| > 2, the field of moduli is a field of definition [CQ05]

If |Aut(C)| = 2, not even a model over \( \mathbb{R} \)

Easy to compute the group of automorphisms of \((E^2, \varphi)\)
(matrices \( P \) such that \( P^* MP = M \))
Models over $\mathbb{Q}$

- If $|\text{Aut}(C)| > 2$, the field of moduli is a field of definition \cite{CQ05}
- If $|\text{Aut}(C)| = 2$, not even a model over $\mathbb{R}$
- Easy to compute the group of automorphisms of $(E^2, \varphi)$
  (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 $\mathbb{Q}$.  

---

Alexandre Gélin  
Principally polarized squares of elliptic curves
Models over $\mathbb{Q}$

- If $|\text{Aut}(C)| > 2$, the field of moduli is a field of definition [CQ05]
- If $|\text{Aut}(C)| = 2$, not even a model over $\mathbb{R}$
- Easy to compute the group of automorphisms of $(E^2, \phi)$
  (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 $\mathbb{Q}$.

Proof

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

Costa-Mascot-Sijsling-Voight (2017)
Thank you