Upper bounds for the endomorphism algebra of an abelian variety

Edgar Costa (MIT)

January 19, 2019
Joint Mathematics Meetings
Joint work with Nicolas Mascot, Jeroen Sijsling, and John Voight

Slides available at `edgarcosta.org` under Research

Elliptic curves

Elliptic curves

$$E : y^2 = x^3 + ax + b, \quad a, b \in \mathbb{Z}$$

Elliptic curves

Elliptic curves

$$E : y^2 = x^3 + ax + b, \quad a, b \in \mathbb{Z}$$

can be split in two classes:

- E is ordinary, i.e., $\mathbf{End}_{\mathbb{Q}} E^{\mathsf{al}} = \mathbb{Q}$,
- E has CM, i.e., $\mathbf{End}_{\mathbb{Q}} E^{\mathsf{al}} = \mathbb{Q}(\sqrt{-d})$ for some $d > 0$

Elliptic curves

Elliptic curves

$$E : y^2 = x^3 + ax + b, \quad a, b \in \mathbb{Z}$$

can be split in two classes:

- E is ordinary, i.e., $\mathbf{End}_{\mathbb{Q}} E^{\mathsf{al}} = \mathbb{Q}$,
- E has CM, i.e., $\mathbf{End}_{\mathbb{Q}} E^{\mathsf{al}} = \mathbb{Q}(\sqrt{-d})$ for some $d > 0$

Warmup problem

How would you distinguish between these two classes?

Approaches

Warmup problem

How would you distinguish between these two classes?

- j-invariant

$$j(E) = 1728\frac{4a^3}{4a^3 + 27b^2}$$

E has CM iff $j(E)$ is in a finite set

Approaches

Warmup problem

How would you distinguish between these two classes?

- j-invariant
$$j(E) = 1728\frac{4a^3}{4a^3 + 27b^2}$$
E has CM iff $j(E)$ is in a finite set
- Embedding it in $\mathbb{C}$
$$E_{\mathbb{C}} \simeq \mathbb{C}/\Lambda, \quad \Lambda = w_1\mathbb{Z} + w_2\mathbb{Z}$$
E has CM iff $w_1/w_2 \in \mathbb{Q}(\sqrt{-d})$ for some $d > 0$

Approaches

Warmup problem

How would you distinguish between these two classes?

- j-invariant
$$j(E) = 1728\frac{4a^3}{4a^3 + 27b^2}$$
E has CM iff $j(E)$ is in a finite set
- Embedding it in $\mathbb{C}$
$$E_{\mathbb{C}} \simeq \mathbb{C}/\Lambda, \quad \Lambda = w_1\mathbb{Z} + w_2\mathbb{Z}$$
E has CM iff $w_1/w_2 \in \mathbb{Q}(\sqrt{-d})$ for some $d > 0$
- Counting points on $E_p := E \bmod p$

$$\mathrm{End}_{\mathbb{Q}}\, E^{\mathrm{al}} \hookrightarrow \mathrm{End}_{\mathbb{Q}}\, E_p^{\mathrm{al}} = \begin{cases} \mathbb{Q}(T)/c_p(T), & \#E_p \neq 1 \bmod p \\ \text{Quaternion alg.}, & \text{otherwise} \end{cases}$$

where $c_p(T) = 1 - (p + 1 - \#E_p)T + pT^2$

Examples

$$\operatorname{End}_{\mathbb{Q}} E^{\mathrm{al}} \hookrightarrow \operatorname{End}_{\mathbb{Q}} E_p^{\mathrm{al}} = \begin{cases} \mathbb{Q}(T)/c_p(T), & \#E_p \neq 1 \bmod p \\ \text{Quaternion alg.}, & \text{otherwise} \end{cases}$$

$E : y^2 + y = x^3 - x^2 - 10x - 20$ **(11.a2)**

- $\operatorname{End}_{\mathbb{Q}} E_2^{\mathrm{al}} \simeq \mathbb{Q}(\sqrt{-1})$
- $\operatorname{End}_{\mathbb{Q}} E_3^{\mathrm{al}} \simeq \mathbb{Q}(\sqrt{-11})$
- $\Rightarrow \operatorname{End}_{\mathbb{Q}} E^{\mathrm{al}} = \mathbb{Q}$

Examples

$$\mathrm{End}_{\mathbb{Q}} E^{\mathrm{al}} \hookrightarrow \mathrm{End}_{\mathbb{Q}} E_p^{\mathrm{al}} = \begin{cases} \mathbb{Q}(T)/c_p(T), & \#E_p \neq 1 \bmod p \\ \text{Quaternion alg.}, & \text{otherwise} \end{cases}$$

$E : y^2 + y = x^3 - x^2 - 10x - 20$ **(11.a2)**

- $\mathrm{End}_{\mathbb{Q}} E_2^{\mathrm{al}} \simeq \mathbb{Q}(\sqrt{-1})$
- $\mathrm{End}_{\mathbb{Q}} E_3^{\mathrm{al}} \simeq \mathbb{Q}(\sqrt{-11})$
- $\Rightarrow \mathrm{End}_{\mathbb{Q}} E^{\mathrm{al}} = \mathbb{Q}$

$E : y^2 + y = x^3 - 7$ **(27.a2)**

- $\mathrm{End}_{\mathbb{Q}} E_p^{\mathrm{al}} = \begin{cases} \text{Quaternion algebra}, & p = 2 \bmod 3 \\ \mathbb{Q}(\sqrt{-3}), & p = 1 \bmod 3 \end{cases}$
- $\rightsquigarrow \mathrm{End}_{\mathbb{Q}} E^{\mathrm{al}} = \mathbb{Q}(\sqrt{-3})$

Genus 2 curves/Abelian surfaces

$$A := \mathrm{Jac}(C : y^2 = a_6 x^6 + \cdots + a_0)$$

Genus 2 curves/Abelian surfaces

$$A := \mathsf{Jac}(C : y^2 = a_6x^6 + \cdots + a_0)$$

There are 6 possibilities for the real endomorphism algebra:

Abelian surface	$\mathsf{End}_{\mathbb{R}}\, A^{\mathsf{al}}$
square of CM elliptic curve	$\mathrm{M}_2(\mathbb{C})$
• QM abelian surface • square of non-CM elliptic curve	$\mathrm{M}_2(\mathbb{R})$
• CM abelian surface • product of CM elliptic curves	$\mathbb{C} \times \mathbb{C}$
product of CM and non-CM elliptic curves	$\mathbb{C} \times \mathbb{R}$
• RM abelian surface • product of non-CM elliptic curves	$\mathbb{R} \times \mathbb{R}$
generic abelian surface	$\mathbb{R}$

Genus 2 curves/Abelian surfaces

$$A := \mathsf{Jac}(C : y^2 = a_6x^6 + \cdots + a_0)$$

There are 6 possibilities for the real endomorphism algebra:

Abelian surface	$\mathsf{End}_{\mathbb{R}}\, A^{\mathsf{al}}$
square of CM elliptic curve	$\mathrm{M}_2(\mathbb{C})$
• QM abelian surface • square of non-CM elliptic curve	$\mathrm{M}_2(\mathbb{R})$
• CM abelian surface • product of CM elliptic curves	$\mathbb{C} \times \mathbb{C}$
product of CM and non-CM elliptic curves	$\mathbb{C} \times \mathbb{R}$
• RM abelian surface • product of non-CM elliptic curves	$\mathbb{R} \times \mathbb{R}$
generic abelian surface	$\mathbb{R}$

Can we distinguish between these by looking at A **mod** p?

Endomorphism algebras over finite fields

Theorem (Tate)

Let A be an abelian variety over $\mathbb{F}_p$, given

$$L_p(T) := \det(1 - t\,\mathrm{Frob}\,|H^1(A)),$$

we may compute $\quad \mathrm{rk}\,\mathrm{End}(A_{\mathbb{F}_{p^r}}), \quad \forall_{r \geq 1}.$

Endomorphism algebras over finite fields

Theorem (Tate)

Let A be an abelian variety over $\mathbb{F}_p$, given

$$L_p(T) := \det(1 - t\,\mathrm{Frob}\,|H^1(A)),$$

we may compute $\mathrm{rk}\,\mathrm{End}(A_{\mathbb{F}_{p^r}}), \quad \forall_{r\geq 1}.$

One can compute $L_p(T)$ by counting points on A

Endomorphism algebras over finite fields

Theorem (Tate)

Let A be an abelian variety over $\mathbb{F}_p$, given

$$L_p(T) := \det(1 - t\,\mathrm{Frob}\,|H^1(A)),$$

we may compute $\quad \mathrm{rk}\,\mathrm{End}(A_{\mathbb{F}_{p^r}}), \quad \forall_{r \geq 1}.$

One can compute $L_p(T)$ by counting points on A

Honda–Tate theory gives us $\mathrm{End}_{\mathbb{Q}}(A_{\mathbb{F}_{p^r}})$ up to isomorphism

Endomorphism algebras over finite fields

Theorem (Tate)

Let A be an abelian variety over $\mathbb{F}_p$, given

$$L_p(T) := \det(1 - t\,\mathrm{Frob}\,|H^1(A)),$$

we may compute $\quad \mathrm{rk}\,\mathrm{End}(A_{\mathbb{F}_{p^r}}), \quad \forall_{r\geq 1}.$

One can compute $L_p(T)$ by counting points on A
Honda–Tate theory gives us $\mathrm{End}_{\mathbb{Q}}(A_{\mathbb{F}_{p^r}})$ up to isomorphism

Example

If $L_5(T) = 1 - 2T^2 + 25T^4$, then

- all endomorphisms are defined over $\mathbb{F}_{25}$;
- $A_{\mathbb{F}_{25}}$ is isogenous to a square of an elliptic curve;
- $\mathrm{End}_{\mathbb{Q}}\, A^{\mathrm{al}} \simeq M_2(\mathbb{Q}(\sqrt{-6}))$

Example continued

$$A = \mathrm{Jac}(y^2 = x^5 - x^4 + 4x^3 - 8x^2 + 5x - 1) \quad (262144.d.524288.1)$$

For $p = 5$, $L_5(T) = 1 - 2T^2 + 25T^4$, and:

- all endomorphisms of A_5 are defined over $\mathbb{F}_{25}$
- $\det(1 - T\,\mathrm{Frob}_5^2 \,|H^1(A)) = (1 - 2T + 25T^2)^2$
- A_5 over $\mathbb{F}_{25}$ is isogenous to a square of an elliptic curve
- $\mathrm{End}_{\mathbb{Q}}\, A_5^{\mathrm{al}} \simeq M_2(\mathbb{Q}(\sqrt{-6}))$

Example continued

$$A = \mathrm{Jac}(y^2 = x^5 - x^4 + 4x^3 - 8x^2 + 5x - 1) \quad (262144.d.524288.1)$$

For $p = 5$, $L_5(T) = 1 - 2T^2 + 25T^4$, and:

- all endomorphisms of A_5 are defined over $\mathbb{F}_{25}$
- $\det(1 - T\,\mathrm{Frob}_5^2 \,|H^1(A)) = (1 - 2T + 25T^2)^2$
- A_5 over $\mathbb{F}_{25}$ is isogenous to a square of an elliptic curve
- $\mathrm{End}_{\mathbb{Q}} A_5^{\mathrm{al}} \simeq M_2(\mathbb{Q}(\sqrt{-6}))$

For $p = 7$, $L_7(T) = 1 + 6T^2 + 49T^4$, and:

- all endomorphisms of A_7 are defined over $\mathbb{F}_{49}$
- $\det(1 - T\,\mathrm{Frob}_7^2 \,|H^1(A)) = (1 + 6T + 49T^2)^2$
- A_7 over $\mathbb{F}_{49}$ is isogenous to a square of an elliptic curve
- $\mathrm{End}_{\mathbb{Q}} A_7^{\mathrm{al}} \simeq M_2(\mathbb{Q}(\sqrt{-10}))$

Example continued

$A = \mathrm{Jac}(y^2 = x^5 - x^4 + 4x^3 - 8x^2 + 5x - 1)$ (262144.d.524288.1)

For $p = 5$, $L_5(T) = 1 - 2T^2 + 25T^4$, and:

- all endomorphisms of A_5 are defined over $\mathbb{F}_{25}$
- $\det(1 - T\,\mathrm{Frob}_5^2 \,|H^1(A)) = (1 - 2T + 25T^2)^2$
- A_5 over $\mathbb{F}_{25}$ is isogenous to a square of an elliptic curve
- $\mathrm{End}_{\mathbb{Q}} A_5^{\mathrm{al}} \simeq M_2(\mathbb{Q}(\sqrt{-6}))$

For $p = 7$, $L_7(T) = 1 + 6T^2 + 49T^4$, and:

- all endomorphisms of A_7 are defined over $\mathbb{F}_{49}$
- $\det(1 - T\,\mathrm{Frob}_7^2 \,|H^1(A)) = (1 + 6T + 49T^2)^2$
- A_7 over $\mathbb{F}_{49}$ is isogenous to a square of an elliptic curve
- $\mathrm{End}_{\mathbb{Q}} A_7^{\mathrm{al}} \simeq M_2(\mathbb{Q}(\sqrt{-10}))$

$\Rightarrow \mathrm{End}_{\mathbb{R}} A^{\mathrm{al}} \neq M_2(\mathbb{C})$

Higher genus

We may factor $\mathbf{End}\, A^{\mathsf{al}}$ uniquely as

$$\mathbf{End}\, A^{\mathsf{al}} \simeq \prod_{i=1}^{t} \mathrm{M}_{n_i}(B_i),$$

where B_i are division algebras

Higher genus

We may factor $\mathsf{End}\, A^{\mathsf{al}}$ uniquely as

$$\mathsf{End}\, A^{\mathsf{al}} \simeq \prod_{i=1}^{t} \mathrm{M}_{n_i}(B_i),$$

where B_i are division algebras with center L_i.
Set $e_i^2 := \mathsf{dim}_{L_i} B_i$, then

$$\mathsf{rk}\, \mathsf{End}(A_K) = \sum_{i=1}^{t} e_i^2 n_i^2 [L_i : \mathbb{Q}].$$

Higher genus

We may factor $\mathsf{End}\, A^{\mathsf{al}}$ uniquely as

$$\mathsf{End}\, A^{\mathsf{al}} \simeq \prod_{i=1}^{t} \mathrm{M}_{n_i}(B_i),$$

where B_i are division algebras with center L_i.
Set $e_i^2 := \mathsf{dim}_{L_i} B_i$, then

$$\mathsf{rk}\, \mathsf{End}(A_K) = \sum_{i=1}^{t} e_i^2 n_i^2 [L_i : \mathbb{Q}].$$

Theorem (C–Mascot–Sijsling–Voight, C–Lombardo–Voight)

We can effectively compute

$$t, \qquad \{e_i n_i\}_{i=1,\dots,t}, \quad \text{and} \quad \{L_i\}_{i=1,\dots,t},$$

if the Mumford–Tate conjecture holds for A.

Higher genus

We may factor $\mathsf{End}\, A^{\mathsf{al}}$ uniquely as

$$\mathsf{End}\, A^{\mathsf{al}} \simeq \prod_{i=1}^{t} \mathrm{M}_{n_i}(B_i),$$

where B_i are division algebras with center L_i.
Set $e_i^2 := \mathsf{dim}_{L_i} B_i$, then

$$\mathsf{rk}\, \mathsf{End}(A_K) = \sum_{i=1}^{t} e_i^2 n_i^2 [L_i : \mathbb{Q}].$$

Theorem (C–Mascot–Sijsling–Voight, C–Lombardo–Voight)

We can effectively compute

$$t, \qquad \{e_i n_i\}_{i=1,\dots,t}, \quad \textit{and} \quad \{L_i\}_{i=1,\dots,t},$$

if the Mumford–Tate conjecture holds for A.

This is done by just counting points.

Real endomorphisms algebras, $\{e_i n_i, n_i \dim A_i\}_{i=1}^t$, and $\dim L_i$

Abelian surface	$\mathsf{End}_{\mathbb{R}} A^{\mathsf{al}}$	tuples	$\dim L_i$
square of CM elliptic crv	$\mathrm{M}_2(\mathbb{C})$	$\{(2,2)\}$	2
• QM abelian surface • square of non-CM elliptic crv	$\mathrm{M}_2(\mathbb{R})$	$\{(2,2)\}$	1
• CM abelian surface	$\mathbb{C} \times \mathbb{C}$	$\{(1,2)\}$	4
• product of CM elliptic crv		$\{(1,1),(1,1)\}$	2, 2
CM $\times$ non-CM elliptic crvs	$\mathbb{C} \times \mathbb{R}$	$\{(1,1),(1,1)\}$	2, 1
• RM abelian surface	$\mathbb{R} \times \mathbb{R}$	$\{(1,2)\}$	2
• prod. of non-CM elliptic crv		$\{(1,1),(1,1)\}$	1, 1
generic abelian surface	$\mathbb{R}$	$\{(1,1)\}$	1

Example continued

$A = \mathrm{Jac}(y^2 = x^5 - x^4 + 4x^3 - 8x^2 + 5x - 1)$ (262144.d.524288.1)

- $\mathrm{End}_{\mathbb{Q}} A_3^{\mathrm{al}} \simeq M_2(\mathbb{Q}(\sqrt{-3}))$
- $\mathrm{End}_{\mathbb{Q}} A_5^{\mathrm{al}} \simeq M_2(\mathbb{Q}(\sqrt{-6}))$
- $\Rightarrow \mathrm{End}_{\mathbb{R}} A^{\mathrm{al}} \neq M_2(\mathbb{C})$

Question

Write $B := \mathrm{End}_{Q} A^{\mathrm{al}}$ and assume that B is a quaternion algr.

Can we guess $\mathrm{disc}\, B$?

Example continued

$A = \mathrm{Jac}(y^2 = x^5 - x^4 + 4x^3 - 8x^2 + 5x - 1)$ (262144.d.524288.1)

- $\mathrm{End}_{\mathbb{Q}} A_3^{\mathrm{al}} \simeq M_2(\mathbb{Q}(\sqrt{-3}))$
- $\mathrm{End}_{\mathbb{Q}} A_5^{\mathrm{al}} \simeq M_2(\mathbb{Q}(\sqrt{-6}))$
- $\Rightarrow \mathrm{End}_{\mathbb{R}} A^{\mathrm{al}} \neq M_2(\mathbb{C})$

Question

Write $B := \mathrm{End}_{Q} A^{\mathrm{al}}$ and assume that B is a quaternion algr.
Can we guess $\mathrm{disc}\, B$?

If ℓ ell is ramified in $B \Rightarrow \ell$ cannot split in $\mathbb{Q}(\mathrm{Frob}_p)$

- $5, 13, 17 \nmid \mathrm{disc}\, B$, as they split in $\mathbb{Q}(\sqrt{-3})$
- $7, 11 \nmid \mathrm{disc}\, B$, as they split in $\mathbb{Q}(\sqrt{-6})$

We can rule out all the primes except 2 and 3 (up to some bnd).

Example continued

$A = \mathrm{Jac}(y^2 = x^5 - x^4 + 4x^3 - 8x^2 + 5x - 1)$ (262144.d.524288.1)

- $\mathrm{End}_{\mathbb{Q}} A_3^{\mathrm{al}} \simeq M_2(\mathbb{Q}(\sqrt{-3}))$
- $\mathrm{End}_{\mathbb{Q}} A_5^{\mathrm{al}} \simeq M_2(\mathbb{Q}(\sqrt{-6}))$
- $\Rightarrow \mathrm{End}_{\mathbb{R}} A^{\mathrm{al}} \neq M_2(\mathbb{C})$

Question

Write $B := \mathrm{End}_{Q} A^{\mathrm{al}}$ and assume that B is a quaternion algr. Can we guess $\mathrm{disc}\, B$?

If ℓ ell is ramified in $B \Rightarrow \ell$ cannot split in $\mathbb{Q}(\mathrm{Frob}_p)$

- $5, 13, 17 \nmid \mathrm{disc}\, B$, as they split in $\mathbb{Q}(\sqrt{-3})$
- $7, 11 \nmid \mathrm{disc}\, B$, as they split in $\mathbb{Q}(\sqrt{-6})$

We can rule out all the primes except 2 and 3 (up to some bnd). Indeed, $\mathrm{disc}\, B = 6$.