Rigorous computation of the endomorphism ring of a Jacobian

Edgar Costa (MIT)

Simons Collab. on Arithmetic Geometry, Number Theory, and Computation

November 13th, 2019

University of New South Wales

Slides available at `edgarcosta.org` under Research

Polynomials

$$f(x) = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$$

Write $f_p(x) := f(x) \bmod p$

- Given $f_p(x)$ what can we say about $f(x)$?

Polynomials

$$f(x) = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$$

Write $f_p(x) := f(x) \bmod p$

- Given $f_p(x)$ what can we say about $f(x)$?
  - factorization of $f_p(x) \rightsquigarrow$
    - factorization of $f(x)$
      e.g.: $f_p(x)$ irreducible $\Rightarrow f(x)$ irreducible
    - factorization of p in $\mathbb{Q}[x]/f(x)$

Polynomials

$$f(x) = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$$

Write $f_p(x) := f(x) \bmod p$

- Given $f_p(x)$ what can we say about $f(x)$?
  - factorization of $f_p(x) \rightsquigarrow$
    - factorization of $f(x)$
      e.g.: $f_p(x)$ irreducible $\Rightarrow$ $f(x)$ irreducible
    - factorization of p in $\mathbb{Q}[x]/f(x)$
- What can we say about $f_p(x)$ for arbitrary p?

Polynomials

$$f(x) = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$$

Write $f_p(x) := f(x) \bmod p$

- Given $f_p(x)$ what can we say about $f(x)$?
  - factorization of $f_p(x) \rightsquigarrow$
    - factorization of $f(x)$
      e.g.: $f_p(x)$ irreducible $\Rightarrow$ $f(x)$ irreducible
    - factorization of p in $\mathbb{Q}[x]/f(x)$
- What can we say about $f_p(x)$ for arbitrary p?
  - For $\deg f = 2$, quadratic reciprocity gives us that

    $$N_f(p) := \#\{\alpha \in \mathbb{F}_p : f_p(\alpha) = 0\}$$

    depending only on $p \bmod \Delta(f)$.

Polynomials

$$f(x) = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$$

Write $f_p(x) := f(x) \bmod p$

- Given $f_p(x)$ what can we say about $f(x)$?
  - factorization of $f_p(x) \rightsquigarrow$
    - factorization of $f(x)$
      e.g.: $f_p(x)$ irreducible $\Rightarrow$ $f(x)$ irreducible
    - factorization of p in $\mathbb{Q}[x]/f(x)$
- What can we say about $f_p(x)$ for arbitrary p?
  - For $\deg f = 2$, quadratic reciprocity gives us that

    $$N_f(p) := \#\{\alpha \in \mathbb{F}_p : f_p(\alpha) = 0\}$$

    depending only on $p \bmod \Delta(f)$.
  - What about for higher degrees?

Polynomials

$$f(x) = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$$

Write $f_p(x) := f(x) \bmod p$

- Given $f_p(x)$ what can we say about $f(x)$?
  - factorization of $f_p(x) \rightsquigarrow$
    - factorization of $f(x)$
      e.g.: $f_p(x)$ irreducible $\Rightarrow$ $f(x)$ irreducible
    - factorization of p in $\mathbb{Q}[x]/f(x)$
- What can we say about $f_p(x)$ for arbitrary p?
  - For $\deg f = 2$, quadratic reciprocity gives us that

    $$N_f(p) := \#\{\alpha \in \mathbb{F}_p : f_p(\alpha) = 0\}$$

    depending only on $p \bmod \Delta(f)$.
  - What about for higher degrees?

$\rightsquigarrow$ studying the **statistical** properties $N_f(p)$.

Example: Cubic polynomials

Theorem (Frobenius)

$$\mathrm{Prob}(N_f(p) = i) = \mathrm{Prob}(g \in \mathrm{Gal}(f) : g \textit{ fixes } i \textit{ roots}),$$

Example: Cubic polynomials

Theorem (Frobenius)

$$\text{Prob}(N_f(p) = i) = \text{Prob}(g \in \text{Gal}(f) : g \textit{ fixes } i \textit{ roots}),$$

$$f(x) = x^3 - 2 = \left(x - \sqrt[3]{2}\right)\left(x - \sqrt[3]{2}e^{2\pi i/3}\right)\left(x - \sqrt[3]{2}e^{4\pi i/3}\right)$$

$$\text{Prob}\left(N_f(p) = k\right) = \begin{cases} 1/3 & \text{if } k = 0 \\ 1/2 & \text{if } k = 1 \\ 1/6 & \text{if } k = 3. \end{cases}$$

$$g(x) = x^3 - x^2 - 2x + 1 = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$$

$$\text{Prob}\left(N_g(p) = k\right) = \begin{cases} 2/3 & \text{if } k = 0 \\ 1/3 & \text{if } k = 3. \end{cases}$$

Example: Cubic polynomials

Theorem (Frobenius)

$$\text{Prob}(N_f(p) = i) = \text{Prob}(g \in \text{Gal}(f) : g \textit{ fixes } i \textit{ roots}),$$

$$f(x) = x^3 - 2 = \left(x - \sqrt[3]{2}\right)\left(x - \sqrt[3]{2}e^{2\pi i/3}\right)\left(x - \sqrt[3]{2}e^{4\pi i/3}\right)$$

$$\text{Prob}\left(N_f(p) = k\right) = \begin{cases} 1/3 & \text{if } k = 0 \\ 1/2 & \text{if } k = 1 \\ 1/6 & \text{if } k = 3. \end{cases} \Rightarrow \text{Gal}(f) = S_3$$

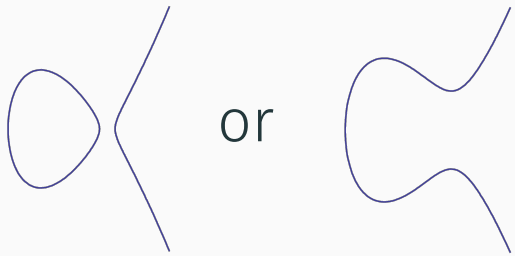
$$g(x) = x^3 - x^2 - 2x + 1 = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$$

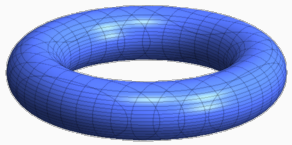
$$\text{Prob}\left(N_g(p) = k\right) = \begin{cases} 2/3 & \text{if } k = 0 \\ 1/3 & \text{if } k = 3. \end{cases} \Rightarrow \text{Gal}(g) = \mathbb{Z}/3\mathbb{Z}$$

Elliptic curves

An *elliptic curve* is a smooth curve defined by

$$y^2 = x^3 + ax + b$$

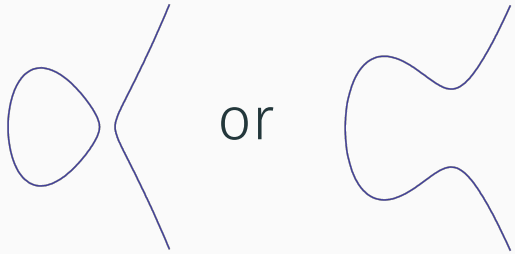
Over $\mathbb{R}$ it might look like  or

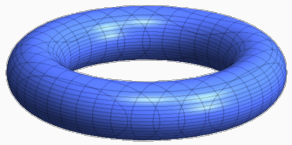
Over $\mathbb{C}$ this is a torus 

Elliptic curves

An *elliptic curve* is a smooth curve defined by

$$y^2 = x^3 + ax + b$$

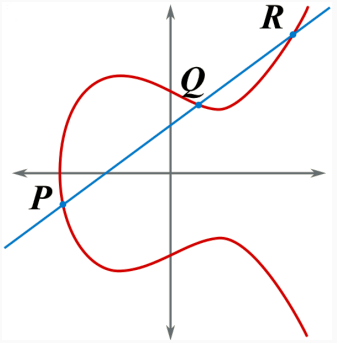
Over $\mathbb{R}$ it might look like  or

Over $\mathbb{C}$ this is a torus 

There is a natural *group structure*!

If P, Q, and R are colinear, then

$$P + Q + R = 0$$



Elliptic curves

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

Elliptic curves

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

Write $E_p := E \bmod p$, for p a prime of good reduction

- What can we say about $\#E_p$ for an arbitrary p?

Elliptic curves

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

Write $E_p := E \bmod p$, for p a prime of good reduction

- What can we say about $\#E_p$ for an arbitrary p?
- Given $\#E_p$ for many p, what can we say about E?

Elliptic curves

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

Write $E_p := E \bmod p$, for p a prime of good reduction

- What can we say about $\#E_p$ for an arbitrary p?
- Given $\#E_p$ for many p, what can we say about E?

$\rightsquigarrow$ studying the **statistical** properties $\#E_p$.

Hasse's bound

Theorem (Hasse, 1930s)

$$|p + 1 - \#E_p| \leq 2\sqrt{p}.$$

Hasse's bound

Theorem (Hasse, 1930s)

$$|p + 1 - \#E_p| \leq 2\sqrt{p}.$$

In other words,

$$\lambda_p := \frac{p + 1 - \#E_p}{\sqrt{p}} \in [-2, 2]$$

What can we say about the error term, λ_p, as $p \to \infty$?

Two types of elliptic curves

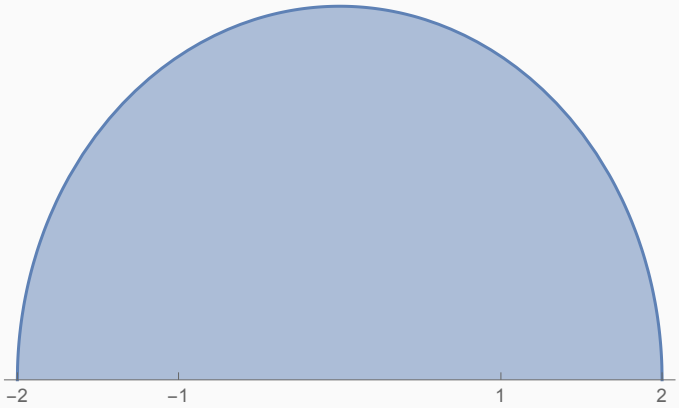
$$\lambda_p := \frac{p + 1 - \#E_p}{\sqrt{p}} \in [-2, 2]$$

There are two limiting distributions for λ_p

Two types of elliptic curves

$$\lambda_p := \frac{p+1-\#E_p}{\sqrt{p}} \in [-2,2]$$

There are two limiting distributions for λ_p



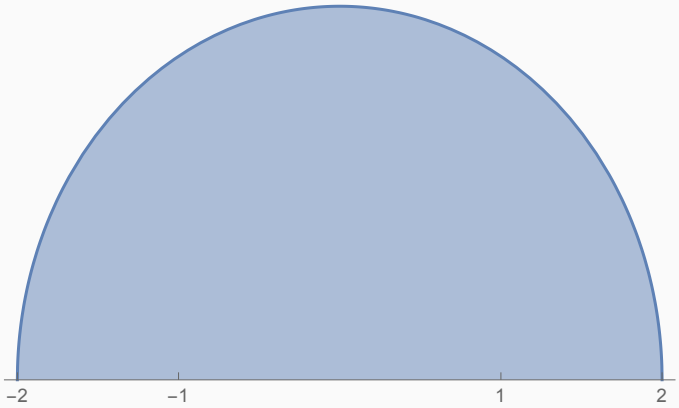
Two types of elliptic curves

$$\lambda_p := \frac{p + 1 - \#E_p}{\sqrt{p}} \in [-2, 2]$$

There are two limiting distributions for λ_p

ordinary

$\mathsf{End}\, E^{\mathsf{al}} = \mathbb{Z}$



special

$\mathsf{End}\, E^{\mathsf{al}} \neq \mathbb{Z}$

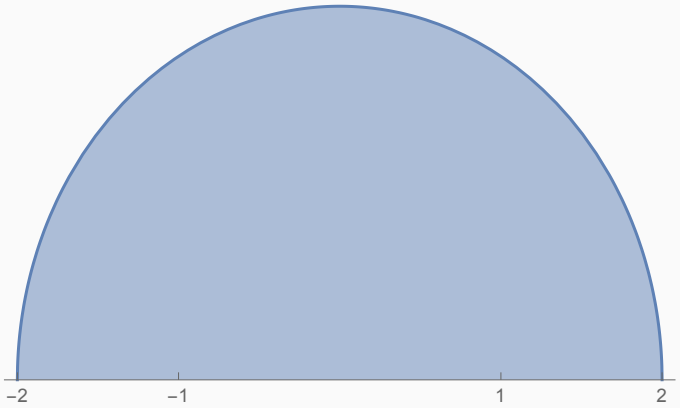
Two types of elliptic curves

$$\lambda_p := \frac{p+1-\#E_p}{\sqrt{p}} \in [-2,2]$$

There are two limiting distributions for λ_p

ordinary

$\mathsf{End}\, E^{\mathsf{al}} = \mathbb{Z}$



$\mathsf{Prob}(\lambda_p = 0) \overset{?}{\sim} 1/\sqrt{p}$

special

$\mathsf{End}\, E^{\mathsf{al}} \neq \mathbb{Z}$

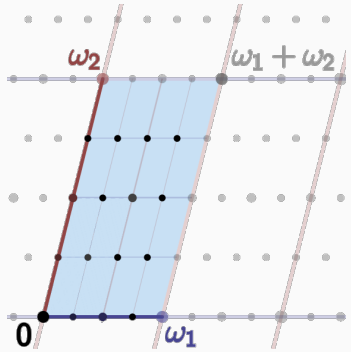
$\mathsf{Prob}(\lambda_p = 0) = 1/2$

Two types of elliptic curves

Over $\mathbb{C}$ an elliptic curve E is a torus

$E_{\mathbb{C}} \simeq \mathbb{C}/\Lambda, \quad$ where $\Lambda = \omega_1\mathbb{Z} + \omega_2\mathbb{Z} =$

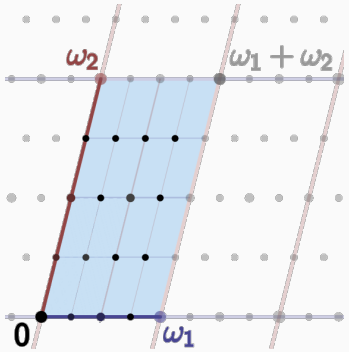
and we have $\mathsf{End}\, E^{\mathsf{al}} = \mathsf{End}\, \Lambda$



Two types of elliptic curves

Over $\mathbb{C}$ an elliptic curve E is a torus

$E_{\mathbb{C}} \simeq \mathbb{C}/\Lambda, \quad$ where $\Lambda = \omega_1\mathbb{Z} + \omega_2\mathbb{Z} =$



and we have $\mathbf{End}\, E^{\mathsf{al}} = \mathbf{End}\, \Lambda$

ordinary

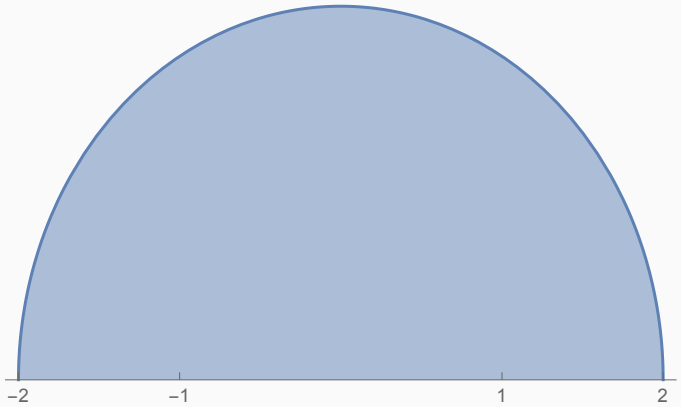
$\mathbf{End}\, \Lambda = \mathbb{Z}$

special

$\mathbb{Z} \subsetneq \mathbf{End}(\Lambda) \subset \mathbb{Q}(\sqrt{-d})$

$\omega_2/\omega_1 \in \mathbb{Q}(\sqrt{-d})$ for some $d > 0$

non-CM

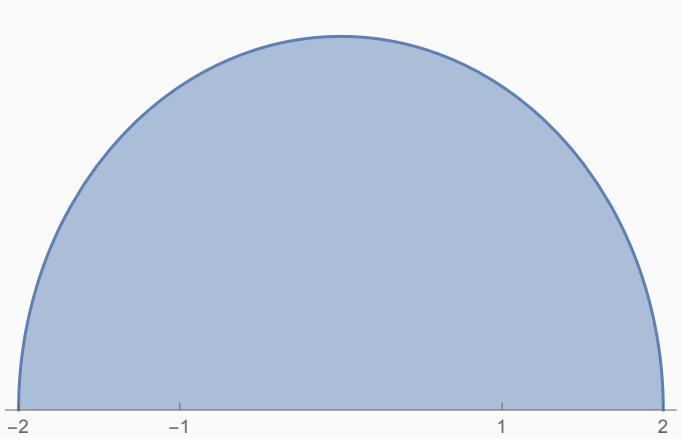


CM

How to distinguish between the two types?

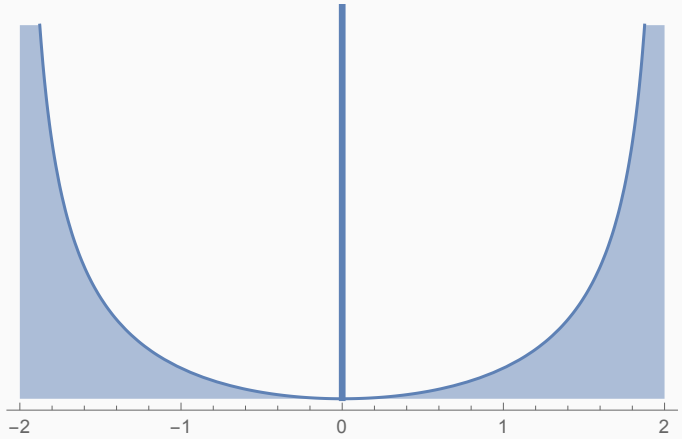
non-CM

$\mathsf{End}_{\mathbb{Q}} E^{\mathsf{al}} = \mathbb{Q}$



CM

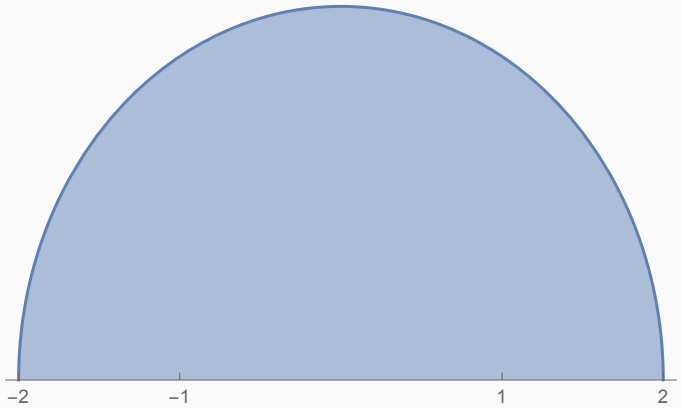
$\mathsf{End}_{\mathbb{Q}} E^{\mathsf{al}} = \mathbb{Q}(\sqrt{-d})$



How to distinguish between the two types?

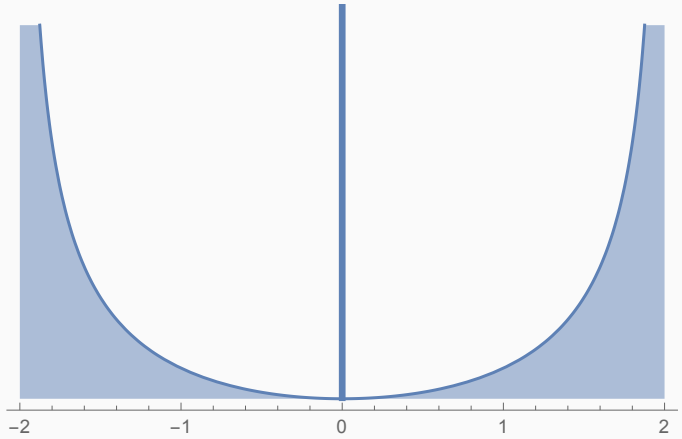
non-CM

$\mathrm{End}_{\mathbb{Q}} E^{\mathrm{al}} = \mathbb{Q}$



CM

$\mathrm{End}_{\mathbb{Q}} E^{\mathrm{al}} = \mathbb{Q}(\sqrt{-d})$



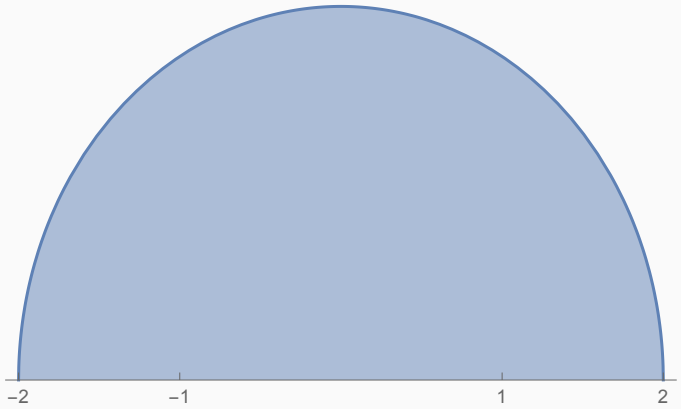
It is enough to count points!

- $p + 1 - \#E_p =: a_p \neq 0 \Longrightarrow \mathrm{End}_{\mathbb{Q}} E^{\mathrm{al}} \subset \mathbb{Q}\left(\sqrt{a_p^2 - 4p}\right)$

How to distinguish between the two types?

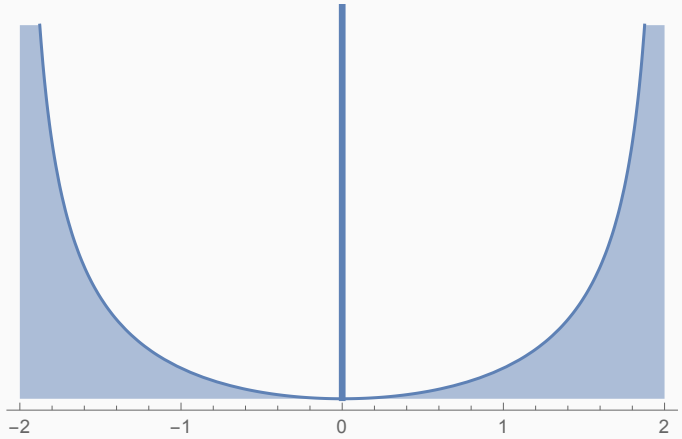
non-CM

$\mathsf{End}_{\mathbb{Q}} E^{\mathsf{al}} = \mathbb{Q}$



CM

$\mathsf{End}_{\mathbb{Q}} E^{\mathsf{al}} = \mathbb{Q}(\sqrt{-d})$



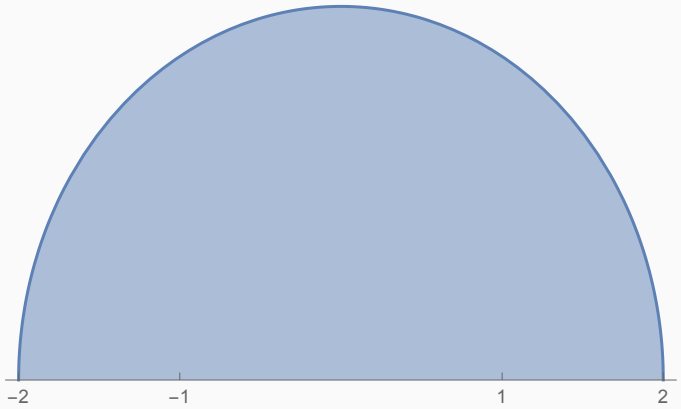
It is enough to count points!

- $p + 1 - \#E_p =: a_p \neq 0 \Longrightarrow \mathsf{End}_{\mathbb{Q}} E^{\mathsf{al}} \subset \mathbb{Q}\left(\sqrt{a_p^2 - 4p}\right)$
- $\mathsf{CM} \Rightarrow \mathbb{Q}(\sqrt{-d}) \simeq \mathbb{Q}\left(\sqrt{a_p^2 - 4p}\right)$.

How to distinguish between the two types?

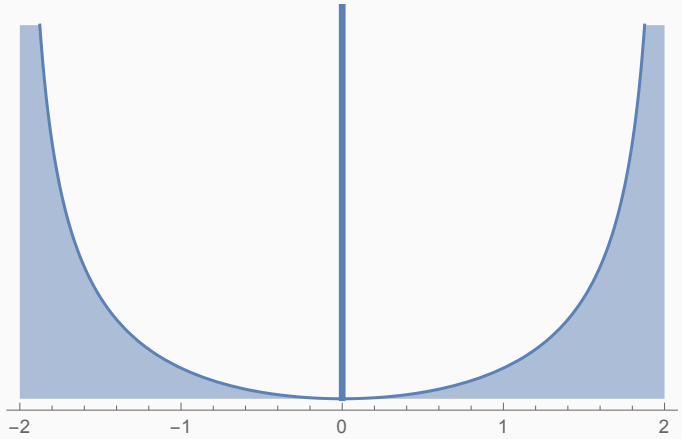
non-CM

$\mathsf{End}_{\mathbb{Q}} E^{\mathsf{al}} = \mathbb{Q}$



CM

$\mathsf{End}_{\mathbb{Q}} E^{\mathsf{al}} = \mathbb{Q}(\sqrt{-d})$



It is enough to count points!

- $p + 1 - \#E_p =: a_p \neq 0 \Longrightarrow \mathsf{End}_{\mathbb{Q}} E^{\mathsf{al}} \subset \mathbb{Q}\left(\sqrt{a_p^2 - 4p}\right)$
- CM $\Rightarrow \mathbb{Q}(\sqrt{-d}) \simeq \mathbb{Q}\left(\sqrt{a_p^2 - 4p}\right)$.
- non-CM $\Rightarrow \mathbb{Q}\left(\sqrt{a_p^2 - 4p}\right) \not\simeq \mathbb{Q}\left(\sqrt{a_q^2 - 4q}\right)$ for $p \neq q$ w/prob 1.

Examples

$$a_p := p + 1 - \#E_p \in [-2\sqrt{p}, 2\sqrt{p}]$$

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

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

Examples

$$a_p := p + 1 - \#E_p \in [-2\sqrt{p}, 2\sqrt{p}]$$

$E : y^2 + y = x^3 - x^2 - 10x - 20$ (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)

- $p = 2 \bmod 3 \Rightarrow a_p = 0 \Rightarrow \mathrm{End}_{\mathbb{Q}} E_p^{\mathrm{al}}$ is a Quaternion algebra
- $p = 1 \bmod 3 \Rightarrow \mathrm{End}_{\mathbb{Q}} E_p^{\mathrm{al}} \simeq \mathbb{Q}(\sqrt{-3})$
- $\rightsquigarrow \mathrm{End}_{\mathbb{Q}} E^{\mathrm{al}} = \mathbb{Q}(\sqrt{-3})$

Group-theoretic interpretation

There is a simple group-theoretic descriptions for these histograms!

Group-theoretic interpretation

There is a simple group-theoretic descriptions for these histograms!

- To E we associate a compact Lie group $\mathrm{ST}_E \subset \mathrm{SU}(2)$
- This group is know as the *Sato–Tate* group of E.
- You may think of it as the “Galois” group of E.

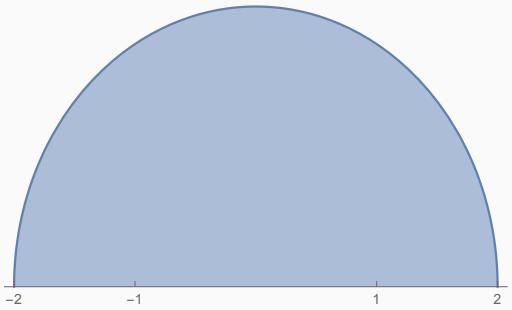
Group-theoretic interpretation

There is a simple group-theoretic descriptions for these histograms!

- To E we associate a compact Lie group $\mathrm{ST}_E \subset \mathrm{SU}(2)$
- This group is know as the *Sato–Tate* group of E.
- You may think of it as the "Galois" group of E.

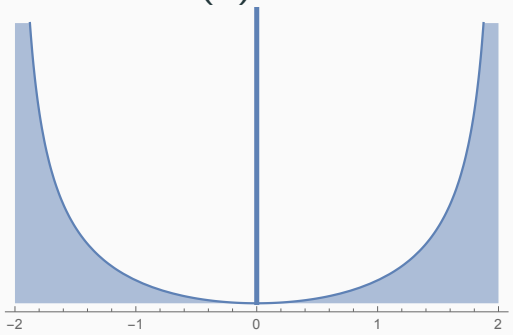
Then, the a_p are distributed as the trace of a matrix chosen at random from ST_E with respect to its Haar measure.

non-CM
$\mathrm{SU}(2)$



CM
$\mathrm{U}(1)$

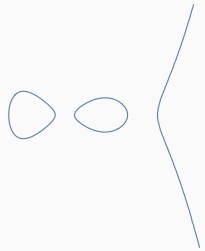
CM (with the δ)
$\mathrm{N}_{\mathrm{SU}(2)}(\mathrm{U}(1))$



Genus 2 curves

An *genus 2 curve* is a smooth curve defined by

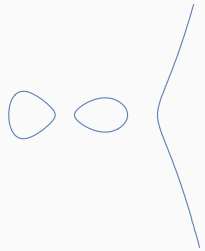
$$y^2 = f(x), \quad \deg f = 5 \text{ or } 6$$

Over $\mathbb{R}$ it might look like 

Genus 2 curves

An *genus 2 curve* is a smooth curve defined by

$$y^2 = f(x), \quad \deg f = 5 \text{ or } 6$$

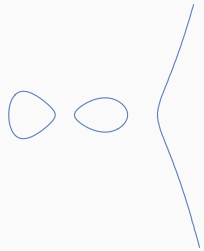
Over $\mathbb{R}$ it might look like 

Now pairs of points have a natural *group structure*

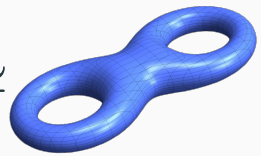
Genus 2 curves

An *genus 2 curve* is a smooth curve defined by

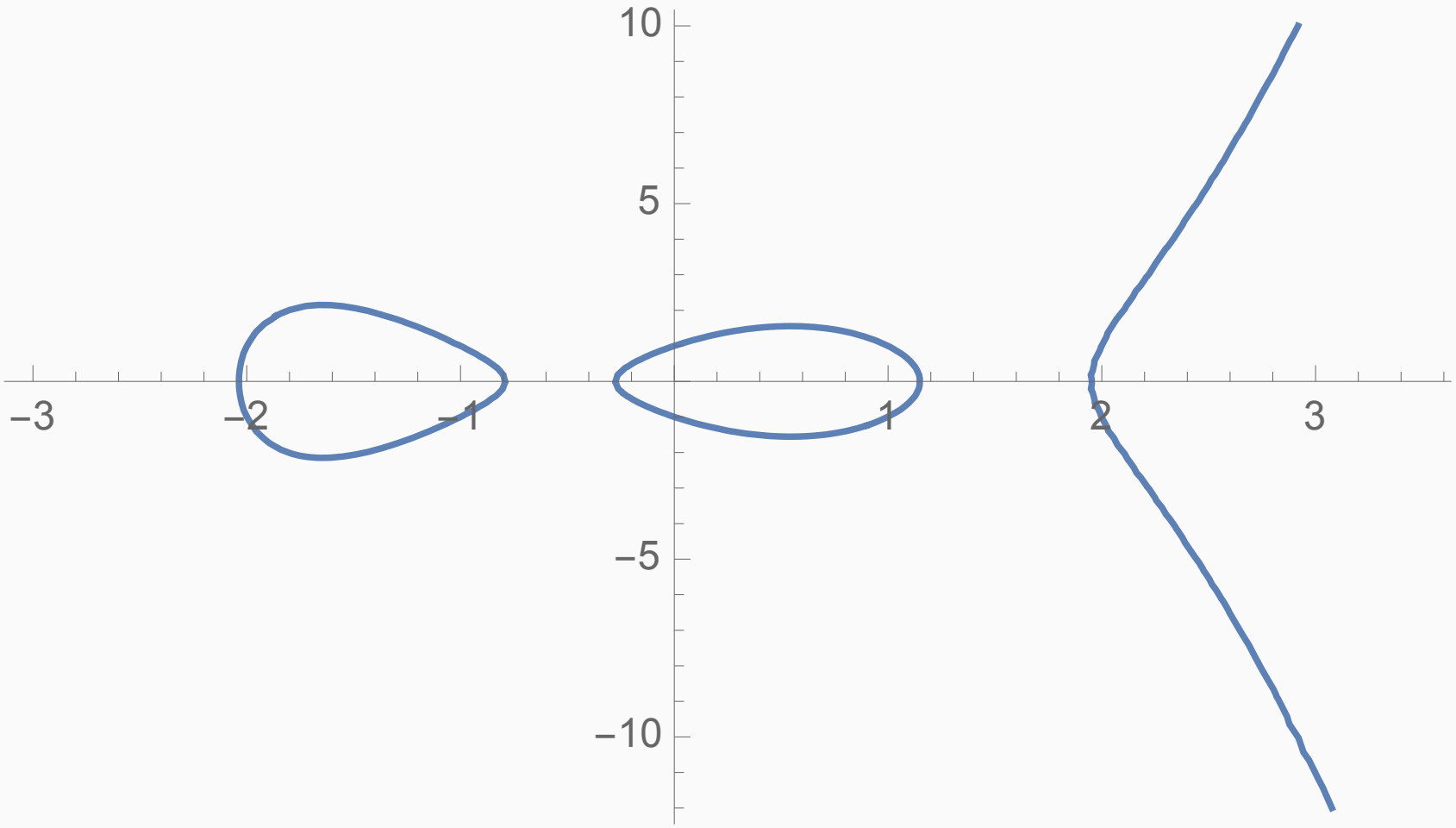
$$y^2 = f(x), \quad \deg f = 5 \text{ or } 6$$

Over $\mathbb{R}$ it might look like 

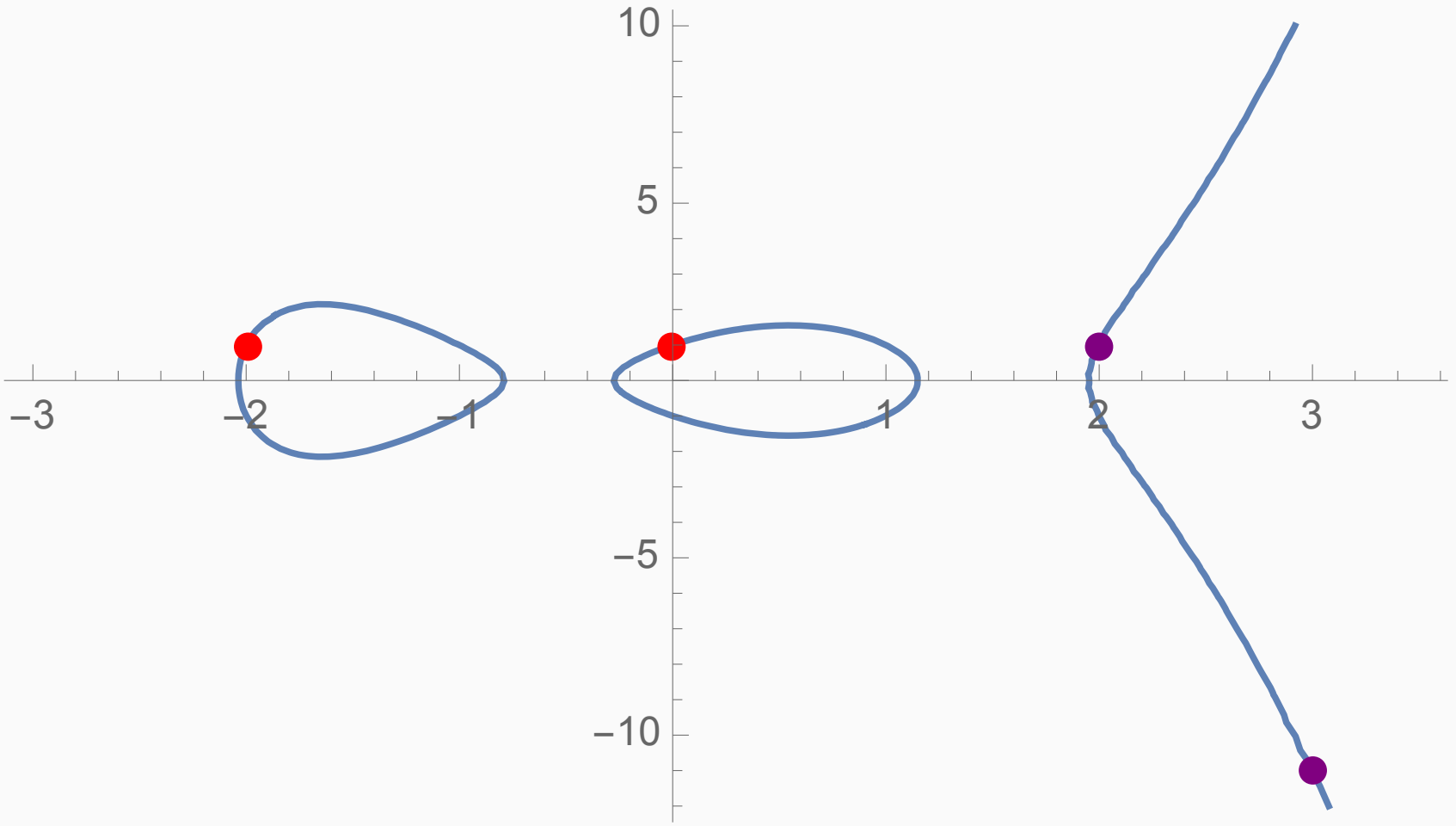
Now pairs of points have a natural *group structure*

Over $\mathbb{C}$ this group structure realizes as $\mathbb{C}^2/\Lambda \simeq$ 

An example, $C : y^2 = x^5 - 5x^3 + 4x + 1$

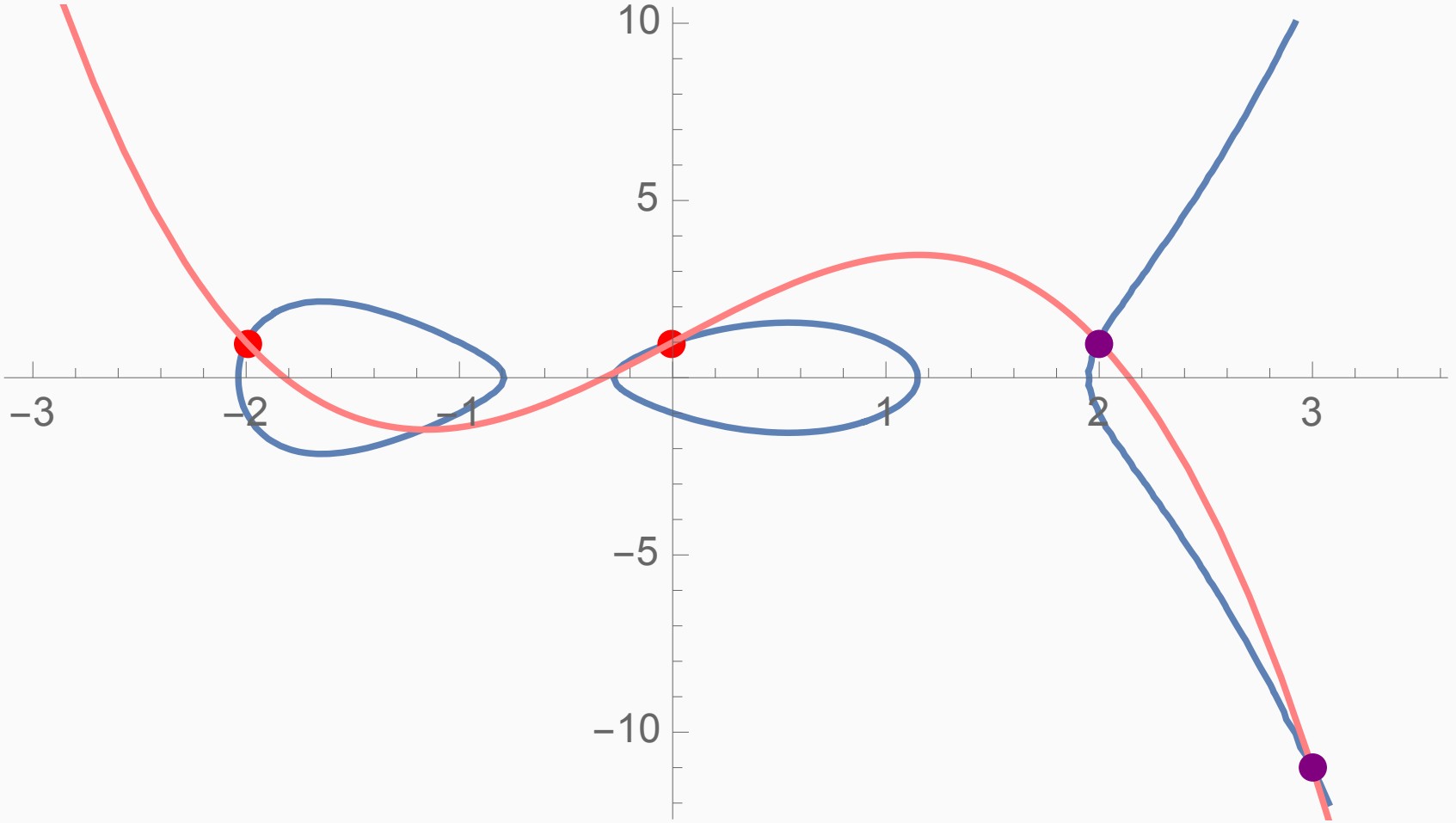


An example, $C : y^2 = x^5 - 5x^3 + 4x + 1$

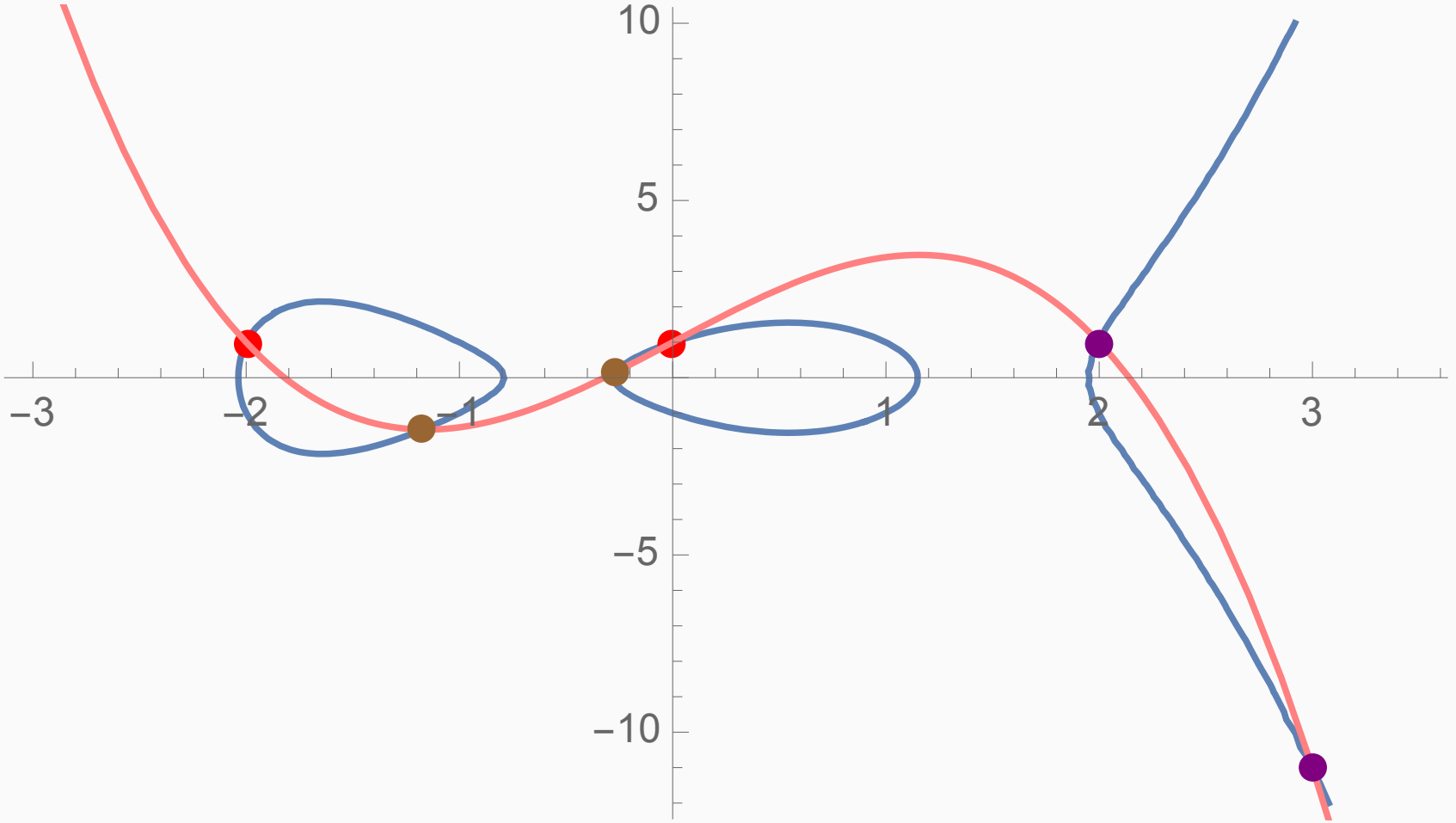


$D_1 := (-2, 1) + (0, 1)$ $D_2 := (2, 1) + (3, -11)$

An example, $C : y^2 = x^5 - 5x^3 + 4x + 1$

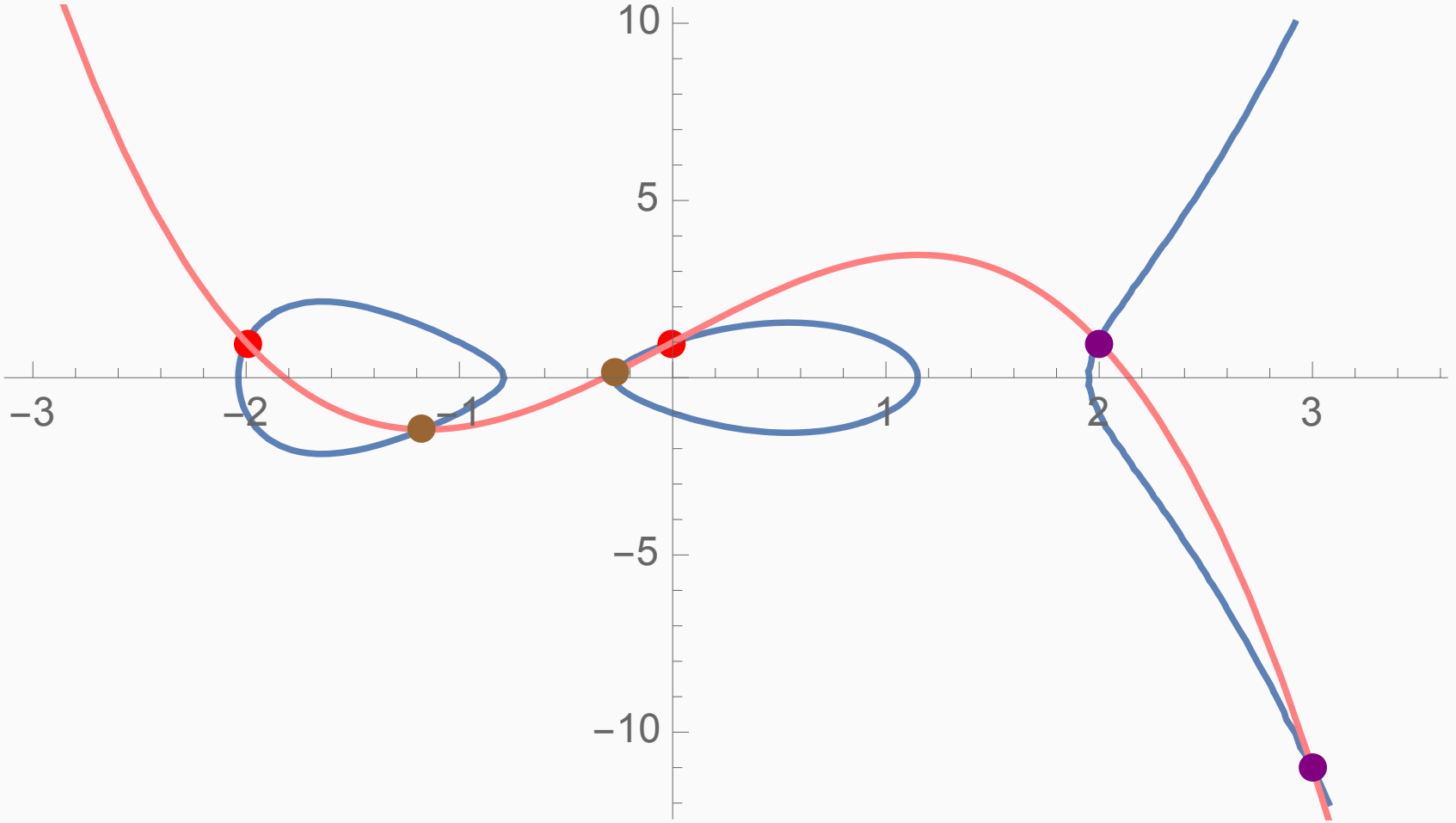


An example, $C : y^2 = x^5 - 5x^3 + 4x + 1$



$$D_3 := \left(\frac{-\sqrt{209}-23}{32}, \frac{-115\sqrt{209}-1333}{2048}\right) + \left(\frac{\sqrt{209}-23}{32}, \frac{115\sqrt{209}-1333}{2048}\right)$$

An example, $C : y^2 = x^5 - 5x^3 + 4x + 1$



$(\bullet + \bullet) + (\bullet + \bullet) + (\bullet + \bullet) = 0$

Real endomorphisms algebras in genus 2

There are 6 possibilities for the real endomorphism algebra[1]:

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	$\mathbb{R}$

[1] and 54 possibilites for Sato–Tate groups

Real endomorphisms algebras in genus 2

There are 6 possibilities for the real endomorphism algebra[1]:

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 $A \bmod p$?

[1] and 54 possibilites for Sato–Tate groups

Zeta functions and Frobenius polynomials

$C/\mathbb{Q}$ a nice curve of genus g and p a prime of good reduction

$$Z_p(T) := \exp\left(\sum_{r=1}^{\infty} \#C(\mathbb{F}_{p^r})T^r/r\right) \in \mathbb{Q}(t)$$

where $\deg L_p(T)$ and

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

where $A := \mathrm{Jac}(C)$.

Zeta functions and Frobenius polynomials

$C/\mathbb{Q}$ a nice curve of genus g and p a prime of good reduction

$$Z_p(T) := \exp\left(\sum_{r=1}^{\infty} \#C(\mathbb{F}_{p^r})T^r/r\right) = \frac{L_p(T)}{(1-T)(1-pT)}$$

where $\deg L_p(T)$ and

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

where $A := \mathrm{Jac}(C)$.

- $g = 1 \rightsquigarrow L_p(T) = 1 - a_pT + pT^2$
- $g = 2 \rightsquigarrow L_p(T) = 1 - a_{p,1}T + a_{p,2}T^2 - a_{p,1}pT^3 + p^2T^4$

Zeta functions and Frobenius polynomials

$C/\mathbb{Q}$ a nice curve of genus g and p a prime of good reduction

$$Z_p(T) := \exp\left(\sum_{r=1}^{\infty} \#C(\mathbb{F}_{p^r})T^r/r\right) = \frac{L_p(T)}{(1-T)(1-pT)}$$

where $\deg L_p(T)$ and

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

where $A := \mathrm{Jac}(C)$.

- $g = 1 \rightsquigarrow L_p(T) = 1 - a_pT + pT^2$
- $g = 2 \rightsquigarrow L_p(T) = 1 - a_{p,1}T + a_{p,2}T^2 - a_{p,1}pT^3 + p^2T^4$

$L_p(T)$ gives us a lot of information about $A_p := A \bmod p$

Endomorphism algebras over finite fields

Theorem (Tate)

Let A be an abelian variety over $\mathbb{F}_q$.

Given $\det(1 - t\,\mathrm{Frob} \mid H^1(A))$, *we may compute* $\mathrm{rk}\,\mathrm{End}(A_{\mathbb{F}_{q^r}}), \forall_{r \geq 1}$.

Endomorphism algebras over finite fields

Theorem (Tate)

Let A be an abelian variety over $\mathbb{F}_q$.

Given $\det(1 - t\,\mathrm{Frob} \mid H^1(A))$, *we may compute* $\mathrm{rk}\,\mathrm{End}(A_{\mathbb{F}_{q^r}}), \forall_{r \geq 1}$.

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

Endomorphism algebras over finite fields

Theorem (Tate)

Let A be an abelian variety over $\mathbb{F}_q$.

Given $\det(1 - t\,\mathrm{Frob} \mid H^1(A))$, *we may compute* $\mathrm{rk}\,\mathrm{End}(A_{\mathbb{F}_{q^r}}), \forall_{r \geq 1}$.

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

Example

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

- all endomorphisms are defined over $\mathbb{F}_{25}$, and
- $A_{\mathbb{F}_{25}}$ 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

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

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

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

Example continued

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

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

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

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

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

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
- $\mathrm{End}_{\mathbb{Q}} A_7^{\mathrm{al}} \simeq M_2(\mathbb{Q}(\sqrt{-10}))$

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

Upper bounds for the endomorphism ring

Let K be a numberfield such that $\mathbf{End}\, A_K = \mathbf{End}\, A^{\mathbf{al}}$

Upper bounds for the endomorphism ring

Let K be a numberfield such that $\mathbf{End}\, A_K = \mathbf{End}\, A^{\mathsf{al}}$, then

- $A_K \sim \prod_{i=1}^{t} A_i^{n_i}$,
- A_i unique and simple up to isogeny (over K),
- $B_i := \mathbf{End}_{\mathbb{Q}}\, A_i$ central simple algebra over $L_i := Z(B_i)$,
- $\mathbf{dim}_{L_i}\, B_i = e_i^2$,
- $\mathbf{End}_{\mathbb{Q}}\, A_K = \prod_{i=1}^{t} M_{n_i}(B_i)$

Upper bounds for the endomorphism ring

Let K be a numberfield such that $\mathbf{End}\, A_K = \mathbf{End}\, A^{\mathsf{al}}$, then

- $A_K \sim \prod_{i=1}^{t} A_i^{n_i}$,
- A_i unique and simple up to isogeny (over K),
- $B_i := \mathbf{End}_{\mathbb{Q}}\, A_i$ central simple algebra over $L_i := Z(B_i)$,
- $\mathbf{dim}_{L_i}\, B_i = e_i^2$,
- $\mathbf{End}_{\mathbb{Q}}\, A_K = \prod_{i=1}^{t} M_{n_i}(B_i)$

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

If Mumford–Tate conjecture holds for A, then we can compute

- t
- $\{(e_i n_i, n_i \,\mathbf{dim}\, A_i)\}_{i=1}^{t}$
- L_i

This is practical and its done by counting points (=computing L_p)

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

Abelian surface	$\mathrm{End}_{\mathbb{R}} A^{\mathrm{al}}$	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 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 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, $\mathrm{disc}\, B = 6$.

Lower bounds for the endomorphism ring

- C be a nice curve of genus g over a number field
- $\mathsf{Jac}(C) \simeq_{\mathbb{C}} \mathbb{C}^g/\Lambda$
- $\mathsf{End}\,\mathsf{Jac}(C)^{\mathsf{al}} \simeq \mathsf{End}\,\mathbb{C}^g/\Lambda \simeq \mathsf{End}\,\Lambda$

Question

Can we compute $\mathsf{End}\,\mathsf{Jac}(C)^{\mathsf{al}}$?

Numerical approach

Question

Can we compute $\mathbf{End}\,\mathrm{Jac}(C)^{\mathrm{al}}$?

$$\mathbf{End}\,\mathrm{Jac}(C)^{\mathrm{al}} \simeq \mathbf{End}\,\mathbb{C}^g/\Lambda \simeq \mathbf{End}\,\Lambda$$

Let the columns of $\Pi \in M_{g,2g}(\mathbb{C})$ be a basis for Λ.

The isomorphism above is realized by

$$M\Pi = \Pi R,$$

where $M \in M_g(\mathbb{Q}^{\mathrm{al}})$ and $R \in M_{2g}(\mathbb{Z})$.

Thus by computing Π, we may compute $\mathbf{End}\,\Lambda$ numerically.

Numerical endomorphism ring (Example continued)

$$C : y^2 = x^5 - x^4 + 4x^3 - 8x^2 + 5x - 1 \quad (262144.d.524288.1)$$

Given Π (with 600 digits)

$$\Pi \approx \begin{pmatrix} 1.851 - 0.1795i & 3.111 + 2.027i & -1.517 + 0.08976i & 1.851 \\ 0.8358 - 2.866i & 0.3626 + 0.1269i & -1.727 + 1.433i & 0.8358 \end{pmatrix}$$

we can verify $\mathsf{Jac}(C)$ has numerical quaternionic multiplication.

For example, we have $\alpha \overset{?}{\in} \mathsf{End}(\mathsf{Jac}(C)_{\mathbb{C}})$ where

$$M_\alpha = \begin{pmatrix} 0 & \sqrt{2} \\ \sqrt{2} & 0 \end{pmatrix} \text{ and } R_\alpha = \begin{pmatrix} 0 & -3 & 0 & -1 \\ -2 & 0 & 1 & 0 \\ 0 & -4 & 0 & -2 \\ 4 & 0 & -3 & 0 \end{pmatrix},$$

which satisfies $\alpha^2 = 2$.

Lower bounds for the endomorphism ring

- C be a nice curve of genus g over a number field
- $\mathsf{Jac}(C) \simeq_{\mathbb{C}} \mathbb{C}^g/\Lambda$
- $\mathsf{End}\,\mathsf{Jac}(C)^{\mathsf{al}} \simeq \mathsf{End}\,\mathbb{C}^g/\Lambda \simeq \mathsf{End}\,\Lambda$

Theorem (C–Mascot–Sijsling–Voight)

There exists a deterministic algorithm that, given input $\alpha \in \mathrm{M}_g(\mathbb{Q}^{\mathsf{al}})$*, returns*

$$\begin{cases} \texttt{true} & \alpha \in \mathsf{End}\,\mathsf{Jac}(C)^{\mathsf{al}} \text{ and } \alpha \text{ is nondegenerate}^2, \\ \texttt{false} & \alpha \notin \mathsf{End}\,\mathsf{Jac}(C)^{\mathsf{al}} \text{ or } \alpha \text{ is degenerate.} \end{cases}$$

[2] i.e., not in the locus of indeterminancy of the Mumford map

Lower bounds for the endomorphism ring

Theorem (C–Mascot–Sijsling–Voight)

There exists a deterministic algorithm that, given input $\alpha \in \mathrm{M}_g(\mathbb{Q}^{\mathrm{al}})$*, returns*

$$\begin{cases} \texttt{true} & \alpha \in \mathsf{End}\,\mathsf{Jac}(C)^{\mathrm{al}} \text{ and } \alpha \text{ is nondegenerate}^3, \\ \texttt{false} & \alpha \notin \mathsf{End}\,\mathsf{Jac}(C)^{\mathrm{al}} \text{ or } \alpha \text{ is degenerate.} \end{cases}$$

Idea:

- α represents an action on the tangent space
- locally this corresponds to system of differential eqns
- solve it locally and match it with a divisor of $C \times C$

[3] i.e., not in the locus of indeterminancy of the Mumford map