Computing central endomorphisms of an abelian variety via reductions modulo p

Edgar Costa (MIT)

January 18, 2020
Joint Mathematics Meetings
Joint work with Davide Lombardo 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 $E_p := E \bmod p$

$$\mathbf{End}_{\mathbb{Q}}\, E^{\mathsf{al}} \hookrightarrow \mathbf{End}_{\mathbb{Q}}\, E_p^{\mathsf{al}} = \begin{cases} \mathbb{Q}(T)/c_p(T), & \#E_p \not\equiv 1 \bmod p \\ \text{Quaternion alg.}, & \text{otherwise} \end{cases}$$

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

Examples

$$\mathrm{End}_{\mathbb{Q}} E^{\mathrm{al}} \hookrightarrow \mathrm{End}_{\mathbb{Q}} E_p^{\mathrm{al}} = \begin{cases} \mathbb{Q}(T)/c_p(T), & \#E_p \not\equiv 1 \bmod p \\ \text{Quaternion alg.}, & \text{otherwise} \end{cases}$$

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

$\mathrm{End}_{\mathbb{Q}} E_2^{\mathrm{al}} \simeq \mathbb{Q}(\sqrt{-1})$

$\mathrm{End}_{\mathbb{Q}} E_3^{\mathrm{al}} \simeq \mathbb{Q}(\sqrt{-11})$

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

Examples

$$\mathrm{End}_{\mathbb{Q}} E^{\mathrm{al}} \hookrightarrow \mathrm{End}_{\mathbb{Q}} E_p^{\mathrm{al}} = \begin{cases} \mathbb{Q}(T)/c_p(T), & \#E_p \not\equiv 1 \bmod p \\ \text{Quaternion alg.}, & \text{otherwise} \end{cases}$$

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

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

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

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

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

$A = \mathsf{Jac}(y^2 = x^5 - x^4 + 4x^3 - 8x^2 + 5x - 1)$ (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
- $\mathrm{End}_{\mathbb{Q}} A_7^{\mathrm{al}} \simeq M_2(\mathbb{Q}(\sqrt{-10}))$

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

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

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

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.

One factor at a time

A an abelian variety over numberfield F

Mumford–Tate conjecture holds for A

$A^{\mathsf{al}} \sim Y^n$, with Y simple, i.e., $\mathsf{End}\, A^{\mathsf{al}} \simeq M_n(B)$

$L := Z(\mathsf{End}_{\mathbb{Q}}\, A^{\mathsf{al}})$

$m^2 := \mathsf{dim}_L\, \mathsf{End}_{\mathbb{Q}}\, A^{\mathsf{al}}$

One factor at a time

A an abelian variety over numberfield F

Mumford–Tate conjecture holds for A

$A^{\mathsf{al}} \sim Y^n$, with Y simple, i.e., $\mathsf{End}\, A^{\mathsf{al}} \simeq M_n(B)$

$L := Z(\mathsf{End}_{\mathbb{Q}}\, A^{\mathsf{al}})$

$m^2 := \mathsf{dim}_L\, \mathsf{End}_{\mathbb{Q}}\, A^{\mathsf{al}}$

Let S be the set of primes $\mathfrak{p}$ of F such that:

(i) A has good reduction at $\mathfrak{p}$

(ii) $A_{\mathfrak{p}} \sim Y^m$ over $\mathbb{F}_{\mathfrak{p}}$ with Y geometrically simple

(iii) $L \hookrightarrow \mathbb{Q}(\mathsf{Frob}_{\mathfrak{p}})$

One factor at a time

A an abelian variety over numberfield F

Mumford–Tate conjecture holds for A

$A^{\mathsf{al}} \sim Y^n$, with Y simple, i.e., $\mathsf{End}\, A^{\mathsf{al}} \simeq M_n(B)$

$L := Z(\mathsf{End}_{\mathbb{Q}}\, A^{\mathsf{al}})$

$m^2 := \mathsf{dim}_L\, \mathsf{End}_{\mathbb{Q}}\, A^{\mathsf{al}}$

Let S be the set of primes $\mathfrak{p}$ of F such that:

(i) A has good reduction at $\mathfrak{p}$

(ii) $A_{\mathfrak{p}} \sim Y^m$ over $\mathbb{F}_{\mathfrak{p}}$ with Y geometrically simple

(iii) $L \hookrightarrow \mathbb{Q}(\mathsf{Frob}_{\mathfrak{p}})$

Theorem (Zywina, C-Lombardo-Voight)

The set S has positive density.

One factor at a time

A an abelian variety over numberfield F
Mumford–Tate conjecture holds for A
$A^{\mathsf{al}} \sim Y^n$, with Y simple, i.e., $\mathsf{End}\, A^{\mathsf{al}} \simeq M_n(B)$
$L := Z(\mathsf{End}_{\mathbb{Q}}\, A^{\mathsf{al}})$
$m^2 := \mathsf{dim}_L\, \mathsf{End}_{\mathbb{Q}}\, A^{\mathsf{al}}$

Let S be the set of primes $\mathfrak{p}$ of F such that:

(i) A has good reduction at $\mathfrak{p}$
(ii) $A_{\mathfrak{p}} \sim Y^m$ over $\mathbb{F}_{\mathfrak{p}}$ with Y geometrically simple
(iii) $L \hookrightarrow \mathbb{Q}(\mathsf{Frob}_{\mathfrak{p}})$

Theorem (Zywina, C-Lombardo-Voight)

The set S has positive density.

If m is unknown, sharp upper bound for m may be obtained.

One factor at a time

Let S be the set of primes $\mathfrak{p}$ of F such that:

(i) A has good reduction at $\mathfrak{p}$

(ii) $A_{\mathfrak{p}} \sim Y^m$ over $\mathbb{F}_{\mathfrak{p}}$ with Y geometrically simple

(iii) $L \hookrightarrow \mathbb{Q}(\mathsf{Frob}_{\mathfrak{p}})$

Theorem (Zywina, C-Lombardo-Voight)

The set S has positive density.

Theorem (C-Lombardo-Voight)

For any $\mathfrak{q} \in S$, and for all $\mathfrak{p} \in S$ outside of a set of density 0 (depending on $\mathfrak{q}$), if $\mathbb{Q}(\mathsf{Frob}_{\mathfrak{q}}) \hookleftarrow M' \hookrightarrow \mathbb{Q}(\mathsf{Frob}_{\mathfrak{p}})$, then $M' \hookrightarrow L$.

How to find L

Let S be the set of primes $\mathfrak{p}$ of F such that:

(i) A has good reduction at $\mathfrak{p}$

(ii) $A_{\mathfrak{p}} \sim Y^m$ over $\mathbb{F}_{\mathfrak{p}}$ with Y geometrically simple
$\Rightarrow \det(1 - T\,\mathrm{Frob}_{\mathfrak{p}} \,|H^1(A)) = g_{\mathfrak{p}}(T)^m, g_{\mathfrak{p}}(T)$ irreducible

(iii) $L \hookrightarrow \mathbb{Q}(\mathrm{Frob}_{\mathfrak{p}})$

Theorem (C-Lombardo-Voight)

For any $\mathfrak{q} \in S$, and for all $\mathfrak{p} \in S$ outside of a set of density 0 (depending on $\mathfrak{q}$), if $\mathbb{Q}(\mathrm{Frob}_{\mathfrak{q}}) \hookleftarrow M' \hookrightarrow \mathbb{Q}(\mathrm{Frob}_{\mathfrak{p}})$, then $M' \hookrightarrow L$.

How to find L

Let S be the set of primes $\mathfrak{p}$ of F such that:

(i) A has good reduction at $\mathfrak{p}$

(ii) $A_{\mathfrak{p}} \sim Y^m$ over $\mathbb{F}_{\mathfrak{p}}$ with Y geometrically simple
$\Rightarrow \det(1 - T\,\mathrm{Frob}_{\mathfrak{p}} \,|H^1(A)) = g_{\mathfrak{p}}(T)^m$, $g_{\mathfrak{p}}(T)$ irreducible

(iii) $L \hookrightarrow \mathbb{Q}(\mathrm{Frob}_{\mathfrak{p}})$

Theorem (C-Lombardo-Voight)

For any $\mathfrak{q} \in S$, and for all $\mathfrak{p} \in S$ outside of a set of density 0 (depending on $\mathfrak{q}$), if $\mathbb{Q}(\mathrm{Frob}_{\mathfrak{q}}) \hookleftarrow M' \hookrightarrow \mathbb{Q}(\mathrm{Frob}_{\mathfrak{p}})$, then $M' \hookrightarrow L$.

There exists an irreducible $h_{\mathfrak{p}}(T) \in L(T)$ such that

$$g_{\mathfrak{p}}(T) = \mathrm{Nm}_{L|\mathbb{Q}}\, h_{\mathfrak{p}}(T)$$

and such that the coefficients of $h_{\mathfrak{p}}(T)$ generate L (over $\mathbb{Q}$).

How to find L

Let S be the set of primes $\mathfrak{p}$ of F such that:

(i) A has good reduction at $\mathfrak{p}$

(ii) $A_{\mathfrak{p}} \sim Y^m$ over $\mathbb{F}_{\mathfrak{p}}$ with Y geometrically simple
$\Rightarrow \det(1 - T\,\mathrm{Frob}_{\mathfrak{p}} \,|H^1(A)) = g_{\mathfrak{p}}(T)^m$, $g_{\mathfrak{p}}(T)$ irreducible

(iii) $L \hookrightarrow \mathbb{Q}(\mathrm{Frob}_{\mathfrak{p}})$

Theorem (C-Lombardo-Voight)

For any $\mathfrak{q} \in S$, and for all $\mathfrak{p} \in S$ outside of a set of density 0 (depending on $\mathfrak{q}$), if $\mathbb{Q}(\mathrm{Frob}_{\mathfrak{q}}) \hookleftarrow M' \hookrightarrow \mathbb{Q}(\mathrm{Frob}_{\mathfrak{p}})$, then $M' \hookrightarrow L$.

There exists an irreducible $h_{\mathfrak{p}}(T) \in L(T)$ such that

$$g_{\mathfrak{p}}(T) = \mathrm{Nm}_{L|\mathbb{Q}}\, h_{\mathfrak{p}}(T)$$

and such that the coefficients of $h_{\mathfrak{p}}(T)$ generate L (over $\mathbb{Q}$).

We can find candidate $h_{\mathfrak{p}}(T)$ by factoring $g_{\mathfrak{p}}(T)$ over $\mathbb{Q}(T)/g_{\mathfrak{q}}(T)$.

How to find L

(i) A has good reduction at $\mathfrak{p}$

(ii) $A_{\mathfrak{p}} \sim Y^m$ over $\mathbb{F}_{\mathfrak{p}}$ with Y geometrically simple

$\Rightarrow \det(1 - T\,\mathrm{Frob}_{\mathfrak{p}} \,|H^1(A)) = g_{\mathfrak{p}}(T)^m$, $g_{\mathfrak{p}}(T)$ irreducible

(iii) $L \hookrightarrow \mathbb{Q}(\mathrm{Frob}_{\mathfrak{p}})$

There exists an irreducible $h_{\mathfrak{p}}(T) \in L(T)$ such that

$$g_{\mathfrak{p}}(T) = \mathrm{Nm}_{L|\mathbb{Q}}\, h_{\mathfrak{p}}(T)$$

and such that the coefficients of $h_{\mathfrak{p}}(T)$ generate L (over $\mathbb{Q}$).

We can find candidate $h_{\mathfrak{p}}(T)$ by factoring $g_{\mathfrak{p}}(T)$ over $\mathbb{Q}(T)/g_{\mathfrak{q}}(T)$. And thus we also obtain candidates for L.

How to find L

(i) A has good reduction at $\mathfrak{p}$

(ii) $A_{\mathfrak{p}} \sim Y^m$ over $\mathbb{F}_{\mathfrak{p}}$ with Y geometrically simple

$\Rightarrow \det(1 - T\,\mathrm{Frob}_{\mathfrak{p}} \,|H^1(A)) = g_{\mathfrak{p}}(T)^m, g_{\mathfrak{p}}(T)$ irreducible

(iii) $L \hookrightarrow \mathbb{Q}(\mathrm{Frob}_{\mathfrak{p}})$

There exists an irreducible $h_{\mathfrak{p}}(T) \in L(T)$ such that

$$g_{\mathfrak{p}}(T) = \mathrm{Nm}_{L|\mathbb{Q}}\, h_{\mathfrak{p}}(T)$$

and such that the coefficients of $h_{\mathfrak{p}}(T)$ generate L (over $\mathbb{Q}$).

We can find candidate $h_{\mathfrak{p}}(T)$ by factoring $g_{\mathfrak{p}}(T)$ over $\mathbb{Q}(T)/g_{\mathfrak{q}}(T)$. And thus we also obtain candidates for L.

With probability one, L is isomorphic to the unique field of maximal degree.

How to find L

(i) A has good reduction at $\mathfrak{p}$

(ii) $A_{\mathfrak{p}} \sim Y^m$ over $\mathbb{F}_{\mathfrak{p}}$ with Y geometrically simple
$\Rightarrow \det(1 - T\,\mathrm{Frob}_{\mathfrak{p}} \,|H^1(A)) = g_{\mathfrak{p}}(T)^m, g_{\mathfrak{p}}(T)$ irreducible

(iii) $L \hookrightarrow \mathbb{Q}(\mathrm{Frob}_{\mathfrak{p}})$

There exists an irreducible $h_{\mathfrak{p}}(T) \in L(T)$ such that

$$g_{\mathfrak{p}}(T) = \mathrm{Nm}_{L|\mathbb{Q}}\, h_{\mathfrak{p}}(T)$$

and such that the coefficients of $h_{\mathfrak{p}}(T)$ generate L (over $\mathbb{Q}$).

We can find candidate $h_{\mathfrak{p}}(T)$ by factoring $g_{\mathfrak{p}}(T)$ over $\mathbb{Q}(T)/g_{\mathfrak{q}}(T)$. And thus we also obtain candidates for L.

With probability one, L is isomorphic to the unique field of maximal degree.

Without Mumford–Tate, this only produces an upper bound.

Summary

Let S be the set of primes $\mathfrak{p}$ of F such that:

(i) A has good reduction at $\mathfrak{p}$

(ii) $A_{\mathfrak{p}} \sim Y^m$ over $\mathbb{F}_{\mathfrak{p}}$ with Y geometrically simple

(iii) $L \hookrightarrow \mathbb{Q}(\mathsf{Frob}_{\mathfrak{p}})$

Theorem (Zywina, C-Lombardo-Voight)

The set S has positive density.

Theorem (C-Lombardo-Voight)

For any $\mathfrak{q} \in S$, and for all $\mathfrak{p} \in S$ outside of a set of density 0 (depending on $\mathfrak{q}$), if $\mathbb{Q}(\mathsf{Frob}_{\mathfrak{q}}) \hookleftarrow M' \hookrightarrow \mathbb{Q}(\mathsf{Frob}_{\mathfrak{p}})$, then $M' \hookrightarrow L$.

Summary

Let S be the set of primes $\mathfrak{p}$ of F such that:

(i) A has good reduction at $\mathfrak{p}$

(ii) $A_{\mathfrak{p}} \sim Y^m$ over $\mathbb{F}_{\mathfrak{p}}$ with Y geometrically simple

(iii) $L \hookrightarrow \mathbb{Q}(\mathsf{Frob}_{\mathfrak{p}})$

Theorem (Zywina, C-Lombardo-Voight)

The set S has positive density.

Theorem (C-Lombardo-Voight)

For any $\mathfrak{q} \in S$, and for all $\mathfrak{p} \in S$ outside of a set of density 0 (depending on $\mathfrak{q}$), if $\mathbb{Q}(\mathsf{Frob}_{\mathfrak{q}}) \hookleftarrow M' \hookrightarrow \mathbb{Q}(\mathsf{Frob}_{\mathfrak{p}})$, then $M' \hookrightarrow L$.

By considering normal closures of $\mathbb{Q}(\mathsf{Frob}_{\mathfrak{p}})$, we obtain similar statements for the splitting field of the Mumford–Tate group.