BUNTES

Angus McAndrew
Dec 8, 2017

The Honda-Tate Theorem

Let $q = p^n$.

Setup: Let A be a simple abelian variety over $\mathbb{F}_q$.
Let π_A be the Frobenius morphism on A.
Let $\mathrm{End}^\circ(A) = \mathbb{Q} \otimes \mathrm{End}(A)$
Let f_A be the characteristic polynomial of π_A.

Some facts: $\mathrm{End}^\circ(A)$ is a division algebra.
$Z(\mathrm{End}^\circ(A)) = \mathbb{Q}(\pi_A)$.
f_A is a power of the minimal polynomial of π_A over $\mathbb{Q}$.

(These are all consequences of the simplicity of A)

Lemma [The Weil Conjectures / Ricky's Theorem]

The roots of f_A all have absolute value $\sqrt{q}$.

Alternate phrasing: $\mathbb{Q}(\pi_A)$ is a number field.
Under every embedding $\iota : \mathbb{Q}(\pi_A) \hookrightarrow \mathbb{C}$ we have $|\iota(\pi_A)| = \sqrt{q}$.

This motivates the following definition.

Def'n: A q-Weil number is an algebraic integer π such that $|\iota(\pi)| = \sqrt{q}$ for all embeddings $\iota : \mathbb{Q}(\pi) \hookrightarrow \mathbb{C}$.

We say q-Weil numbers π, π' are conjugate if they have the same minimal polynomial over $\mathbb{Q}$, and write $\pi \sim \pi'$.

Thus, from what has been discussed so far we have a map

$$\{\text{Simple AVs over } \mathbb{F}_q\} \longrightarrow \{q\text{-Weil numbers}\}$$

$$A \longmapsto \pi_A.$$

Our goal for today is to prove the following

Theorem [Honda-Tate]

We have a bijection

$$HT: \left\{\begin{array}{l}\text{Isogeny classes of} \\ \text{simple AVs over } \mathbb{F}_q\end{array}\right\} \xrightarrow{\sim} \left\{\begin{array}{l}\text{Conjugacy classes of} \\ q\text{-Weil numbers}\end{array}\right\}$$

$$A \longmapsto \pi_A$$

First we will show this map is well-defined (a simple corollary of Tate's theorem).

Injectivity will require additional knowledge of the endomorphism algebras of simple abelian varieties.

Surjectivity (i.e. constructing AVs from q-Weil numbers) will be the bulk of our work.

Recall the following corollary of Tate's Theorem from last time.

Corollary: Let A, B be AVs over $\mathbb{F}_q$ with rational Tate modules $V_\ell A$, $V_\ell B$ for $\ell \neq p$.

Then

$$A \underset{\text{isogenous}}{\sim} B \iff V_\ell A \cong V_\ell B \quad \forall \ell \neq p.$$

From this we deduce the following.

Corollary: $A \underset{\text{isog}}{\sim} B \iff f_A = f_B$

Pf: ($\Rightarrow$) f_A is the characteristic polynomial of $V_\ell(\pi_A)$ acting on $V_\ell A$ (similarly for f_B).

Thus

$$V_\ell A \cong V_\ell B \Rightarrow f_A = f_B.$$

($\Leftarrow$) $V_\ell A$ and $V_\ell B$ are semisimple Galois representations

Thus, by the Brauer-Nesbitt Theorem they can be recovered from the characteristic polynomials f_A, f_B.

Thus

$$f_A = f_B \Rightarrow V_\ell A \cong V_\ell B \quad \forall \ell \neq p. \qquad \square$$

So we now have

$$A \underset{\text{isog}}{\sim} B \Rightarrow \text{minpoly}(\pi_A) = \text{minpoly}(\pi_B)$$

$$\Rightarrow \pi_A, \pi_B \text{ are conjugate as } q\text{-Weil numbers.}$$

So we now have a well-defined function

$$HT: \left\{ \begin{array}{l} \text{Isogeny classes of} \\ \text{Simple AVs over } \mathbb{F}_q \end{array} \right\} \longrightarrow \left\{ \begin{array}{l} \text{Conjugacy classes of} \\ q\text{-Weil numbers} \end{array} \right\}$$

$$A \mapsto \pi_A$$

We now need bijectivity.

Injectivity and Brauer Groups

Given π_A, π_B conjugate, we know they have the same minimal polynomial over $\mathbb{Q}$.

We need to show that for A simple, we can recover f_A from π_A (that is, take the correct power of the minimal polynomial).

Last time: There exists a certain quantity $r(f, g)$ such that

$$r(f_A, f_B) = \operatorname{rank} \operatorname{Hom}(A, B)$$

Corollary: Let $d = [\operatorname{End}^0(A) : \mathbb{Q}(\pi_A)]^{1/2}$.
Let h_A be the minimal polynomial of π_A over $\mathbb{Q}$.
Then $f_A = h_A^d$.

Pf: Study formula for $r(f_A, f_A)$, given in [B-vdG-M] Lemma 16.22. □

So if we can construct the division algebra $\operatorname{End}^0(A)$ from π_A, we are done.

Dfn: A central simple algebra over a field k is an finite dim k-algebra with no two-sided ideals and centre k.

Thm (Artin-Wedderburn) Any finite dimensional simple k-algebra is isomorphic to $M_n(D)$ for D a division k-algebra.

Dfn: The Brauer group of a field k, denoted $Br(k)$ is the set of central simple algebras over k under tensor product, modulo the algebras $M_n(k)$.

Facts:
- $\bar{k} = k \Rightarrow Br(k) = 0$
- k complete nonarchimedean $\Rightarrow Br(k) = \mathbb{Q}/\mathbb{Z}$
- $Br(\mathbb{R}) = \mathbb{Z}/2\mathbb{Z}$

Given a place v of k we get a map

$$\begin{aligned} Br(k) &\longrightarrow Br(k_v) \\ D &\longmapsto D \otimes_k k_v \end{aligned}$$

In fact we have an injection

$$Br(k) \hookrightarrow \prod_v Br(k_v) \simeq \prod_{v \text{ nonarch}} \left(\mathbb{Q}/\mathbb{Z}\right) \times \prod_{v \text{ real}} \mathbb{Z}/2\mathbb{Z}$$

$$D \longmapsto (D \otimes_k k_v)_v \longmapsto (inv_v(D))_v$$

These $inv_v(D)$ are called the local invariants of D.

Proposition: Let $A/\mathbb{F}_q$ be an elementary abelian variety.
Let $K = \mathbb{Q}(\pi_A)$.
Then

$$\mathrm{inv}_v(\mathrm{End}^0(A)) = \begin{cases} \frac{\mathrm{ord}_v(\pi_A)}{\mathrm{ord}_v(q)} \in \frac{1}{[K:\mathbb{Q}_p]}\mathbb{Z}, & v \mid p \\ 1/2, & v \text{ real} \\ 0, & v \nmid p \text{ finite or } v \text{ complex} \end{cases}$$

[E-M-vdG, Cor 16.38].

Proposition: A as above, let $d = [\mathrm{End}^0(A) : \mathbb{Q}(\pi_A)]^{1/2}$ as before.
Then d is the least common denominator of $\{\mathrm{inv}_v(\mathrm{End}^0(A))\}_v$.

Corollary: $\pi_A \sim \pi_B \iff f_A = f_B$.

Pf: ($\Leftarrow$) ✓

($\Rightarrow$) Let $h = \mathrm{minpoly}(\pi_A) = \mathrm{minpoly}(\pi_B)$.
Then $f_A = h^d$, $f_B = h^{d'}$.
Let $K = \mathbb{Q}(\pi_A) = \mathbb{Q}(\pi_B)$
Let D_{π_A}, D_{π_B} be the division Kalgebras specified by the local invariants above, which are determined by π_A, π_B.
However, since $\pi_A \sim \pi_B$, $\mathrm{inv}_v(D_{\pi_A}) = \mathrm{inv}_v(D_{\pi_B})$.

$\Rightarrow d = d'$
$\Rightarrow f_A = f_B$. □

Corollary: HT is injective.

Surjectivity

This is the main hurdle in proving the Honda-Tate theorem. We must show that for any q-Weil number π there exists an abelian variety A over $\mathbb{F}_q$ such that $\pi_A \sim \pi$.

Language: We say π is effective if it is in the image of HT.

We first make a reduction.

Proposition: Let $N \in \mathbb{Z}_{\geq 1}$.
If π^N is effective, then π is effective.

Pf: Let k be a degree N extension of $\mathbb{F}_q$.
By assumption we have A' a simple abelian variety over k such that $\pi^N \sim \pi_{A'}$.
Let

$$A = \mathrm{Res}_{k'/\mathbb{F}_q}(A').$$

On the rational Tate modules we have

$$V_\ell A = \mathrm{Ind}_{G_k}^{G_{\mathbb{F}_q}} V_\ell A'$$

where $G_k = \mathrm{Gal}(\overline{\mathbb{F}}_p/k)$, $G_{\mathbb{F}_q} = \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_q)$.

(This follows from functoriality of Weil restriction).

By noting that G_k, $G_{\mathbb{F}_q}$ are abelian and studying the precise actions, one can see that

$$\mathrm{Ind}_{G_k}^{G_{\mathbb{F}_q}}(\pi_{A'}) = \pi_A^N \quad \text{acting on} \quad \mathrm{Ind}_{G_k}^{G_{\mathbb{F}_q}}(V_\ell A').$$

Thus $\mathrm{Res}_{k/\mathbb{F}_q}(\pi_{A'}) = \pi_A^N$.

In particular we see $f_A(T) = f_{A'}(T^N)$.

In general, A will not be simple.
We can choose a simple factor A_i on which we have π_{A_i} and f_{A_i}.
Since $f_{A_i} \mid f_A$, we conclude $\pi_{A_i} \sim \pi$. □

From this it is sufficient to show that π^N is effective for some N.

Strategy from here:

1. Construct division algebra D_π
2. Choose CM field L splitting D
3. Find abelian variety A/Φ of type (L, Φ)
4. A is in fact defined over a number field K and has good reduction at $v \mid p$
5. Apply the Taniyama–Shimura formula to relate π_A to Φ
6. Choose Φ wisely in (3) (in retrospect) to relate π and π_A
7. Show $\pi^N \sim \pi_A^N$.

(1) D_π is constructed as when we proved injectivity, using the local invariants coming from the Brauer group.

(2)

Dfn: A CM field is a number field $L/\mathbb{Q}$ such that there is a totally real $K/\mathbb{Q}$ with L/K totally imaginary quadratic.

Prop: Let π be a q-Weil number.
There exists a CM field $L/\mathbb{Q}(\pi)$ such that L splits D_π (ie $L \otimes_{\mathbb{Q}(\pi)} D_\pi$ is a matrix algebra over L), and further $[L:\mathbb{Q}(\pi)] = [D_\pi : \mathbb{Q}(\pi)]^{1/2}$.

Pf: For a q-Weil number π, either
(a) $\mathbb{Q}(\pi)$ totally real, then $\mathbb{Q}(\pi) = \mathbb{Q}$ or $\mathbb{Q}(\sqrt{p})$
(b) $\mathbb{Q}(\pi)$ a CM field with totally real subfield $\mathbb{Q}(\pi + q/\pi)$.

In the case
(a) Let $L = \mathbb{Q}(\pi)(\sqrt{-p})$.
Since $[L:\mathbb{Q}(\pi)] = 2$, this doubles the invariant at v thus splits D_π.
(b) Let $d = [D_\pi : \mathbb{Q}(\pi)]^{1/2}$.
We can find $L/\mathbb{Q}(\pi)$ such that for every $v|p$ the local degree is d (by weak approximation).
Tensoring up to L will thus clear denominators in $\mathbb{Q}/\mathbb{Z}$ and split D_π.

□

③ For a CM field L, all its embeddings $\iota : L \to \mathbb{C}$ come in complex conjugate pairs.
For each pair, choose one embedding.
We thus get a subset $\Phi \subseteq \mathrm{Hom}(L, \mathbb{C})$ with the properties

$$\Phi \cup \overline{\Phi} = \mathrm{Hom}(L, \mathbb{C})$$
$$\Phi \cap \overline{\Phi} = \emptyset.$$

Such a choice of Φ is a <u>CM type</u>.

Let $A/\mathbb{C}$ be an abelian variety with CM by L (i.e. a map $L \to \mathrm{End}^0(A)$).
Then $\mathbb{C} \otimes_{\mathbb{Q}} L = \prod_{\iota \in \mathrm{Hom}(L,\mathbb{C})} \mathbb{C}$ acts on the tangent space at the origin, $\mathrm{Lie}(A)$.

<u>Prop</u>: The action of $\mathbb{C} \otimes_{\mathbb{Q}} L$ on $\mathrm{Lie}(A)$ factors through the quotient $\prod_{\iota \in \Phi} \mathbb{C}$ for some CM type (L, Φ).

A is then said to be of type (L, Φ).

<u>Theorem</u>: Let (L, Φ) be a CM type.
There exists an abelian variety $A/\mathbb{C}$ of type (L, Φ).

<u>Pf</u>: This is a result from CM theory for AVs.
It's in Shimura-Taniyama (possibly due to them?)

□

④ The fact that A is in fact defined over some number field K is also in Shimura-Taniyama.

Thm: Let A/k be an abelian variety over a number field which admits CM.
Then A admits potentially good reduction at all places v of K (ie. good reduction after passing to a finite extension).

Pf: Highly nontrivial, uses Néron Models, Chevalley Decomposition, Néron-Ogg-Shafarevich, and a result of Grothendieck on potentially stable reduction. □

After passing to a finite extension, we can assume A has good reduction at $v|p$ and thus we have the reduction over $\mathbb{F}_{q'}$, denoted $A_{\mathbb{F}_{q'}}$.

⑤ For a place w of our CM field L, let
$\Sigma_w = \mathrm{Hom}(L_w, \mathbb{C}_p)$
$\Phi_w = \Phi \cap \Sigma_w$.

Theorem [Shimura-Taniyama Formula]
For all places $w|p$ of L, $\dfrac{\omega(\pi_{A_{\mathbb{F}_q}})}{\omega(q)} = \dfrac{\#\Phi_w}{\#\Sigma_w}$.

Pf: Tate gives a proof using "CM theory of p-divisible groups". □

(6) Recall we have fixed π, and this deterministically fixed $Q(\pi)$, D_π and L.

However, we have had no restrictions on our choice of Φ.

Lemma: We can choose Φ such that for all places $w|p$ of L,

$$\frac{w(\pi)}{w(q)} = \frac{\#\Phi_w}{\#\Sigma_w}$$

Proof: Let $v = w|_{Q(\pi)}$ be the place of $Q(\pi)$ below w.

Let

$$n_w = \frac{w(\pi)}{w(q)} \cdot \#\Sigma_w = \frac{w(\pi)}{w(q)} [L_w : \mathbb{Q}_p]$$

$$= \frac{w(\pi)}{w(q)} [L_w : Q(\pi)_v][Q(\pi)_v : \mathbb{Q}_p]$$

Then, by recalling the formula for the local invariants of D_π we see

$$n_w = inv_w (D_\pi \otimes_{Q(\pi)} L).$$

However, since L splits $D_\pi \Rightarrow n_w \in \mathbb{Z}$.

Further

$$n_w + n_{\bar{w}} = \left(\frac{w(\pi)}{w(q)} + \frac{w(\bar{\pi})}{w(q)}\right) \#\Sigma_w$$

$$= \frac{w(\pi\bar{\pi})}{w(q)} \#\Sigma_w = \frac{w(q)}{w(q)} \#\Sigma_w = \#\Sigma_w$$

We can choose a CM type $\Phi = \bigcup_w \Phi_w$ where for each w we have $\#\Phi_w = n_w$.

Then the result follows. □

(7) We now have an abelian variety $A/\mathbb{F}_q$ of type (L, Φ) such that for all places $w|p$ of L,

$$\frac{w(\pi_A)}{w(q')} = \frac{w(\pi)}{w(q)}$$

Proposition: With the above, there exist $N, N' \in \mathbb{Z}_{\geq 1}$ such that

$$\pi_A^N = \pi^{N'}.$$

Proof: Choose $m, m' \in \mathbb{Z}_{\geq 1}$ such that $(q')^m = q^{m'}$.

Then

$$\frac{w(\pi_A^m)}{w((q')^m)} = \frac{w(\pi^{m'})}{w(q^{m'})}$$

$$\Rightarrow w(\pi_A^m) = w(\pi^{m'})$$

$$\Rightarrow w\left(\frac{\pi_A^m}{\pi^{m'}}\right) = 1 \qquad \forall\, w|p$$

Since $\pi_A^m, \pi^{m'} \mid q^{m'}$, for $w \nmid p$ they are units.

Finally $|\pi_A^m| = |\pi^{m'}| = \sqrt{q^{m'}}$ at infinite places.

$$\Rightarrow w\left(\frac{\pi_A^m}{\pi^{m'}}\right) = 1 \qquad \forall\, w$$

$$\Rightarrow \pi_A^m / \pi^{m'} \text{ is a root of unity}$$

$$\Rightarrow \pi_A^N / \pi^{N'} = 1$$

□

Wrapping up: Thus $\pi^{N'}$ is effective for some N'.

$\Rightarrow \pi$ is effective

$\Rightarrow$ HT is surjective (so bijective).

Remarks: Honda's paper essentially deals with aspects ⑥ and ⑦, but with a totally different approach to the one here.

References:
- Edixhoven - van der Geer - Moonen
- Eisenträger, "Thm of Honda and Tate"
- Oort
- Lawrence, "Surjectivity in Honda-Tate"
- Shimura - Taniyama, "CM of AVs and application to Number Theory"
- Honda, "Isogeny classes of AVs over finite fields"