# An example of the Honda-Tate theorem

Ravi Fernando – fernando@berkeley.edu

August 17, 2018

Given an abelian variety $A$ of dimension $g$ over a finite field $\mathbb{F}_q$, we can associate to $A$ a multiset of $2g$ algebraic numbers, the eigenvalues of $\mathrm{Frob}_q$ on $H^1_{\text{ét}}(A_{\overline{\mathbb{F}_q}}, \mathbb{Q}_\ell)$ for any $\ell \nmid q$. These are all Weil $q$-integers; that is, they are algebraic integers with absolute value $\sqrt{q}$ upon any embedding into $\mathbb{C}$. It is well-known that isogenous abelian varieties have the same Frobenius eigenvalues, and that the Frobenius eigenvalues of a simple abelian variety form a single Galois conjugacy class (possibly with multiplicity—more on this soon). This allows us to state the Honda-Tate theorem:

**Theorem 1.** *(Honda-Tate) For every finite field $\mathbb{F}_q$, the map*

$$\{\textit{simple abelian varieties over } \mathbb{F}_q\}/\textit{isogeny} \longrightarrow \{G_{\mathbb{Q}}\textit{-conjugacy classes of Weil } q\textit{-numbers}\}$$

*is a bijection.*

Injectivity was proved by Tate in 1966, and surjectivity by Honda in 1968.

One might naively expect that for abelian varieties of dimension $g$, the resulting Frobenius eigenvalues $\alpha_1, \ldots, \alpha_{2g}$ are all distinct algebraic integers of degree $2g$. Indeed, they are all roots of the characteristic polynomial $f_A(x) = \prod_{i=1}^{2g}(x - \alpha_i)$, which is in $\mathbb{Z}[x]$ by the "rationality" Weil conjecture. Moreover, if $B$ is another abelian variety with $f_B | f_A$, then $B$ embeds into $A$ up to isogeny. (The isogeny category is semisimple, so in this case $A$ is isogenous to the direct product of $B$ and some other abelian variety $B'$.) But it is nonetheless possible for $f_A(x)$ to be reducible even when $A$ is simple. The purpose of this note is to illustrate a concrete example of this type of behavior. This example was worked out with Sander Mack-Crane and Dylan Yott after Berkeley's RTG research workshop on arithmetic geometry in spring 2018.

Let us begin by illustrating an example of the "expected" behavior. Fix a prime $p$. If $E/\mathbb{F}_p$ is an elliptic curve with Frobenius eigenvalues $\alpha_1, \alpha_2$, we have $|E(\mathbb{F}_{p^n})| = 1 + p^n - \alpha_1^n - \alpha_2^n$. In particular, $|E(\mathbb{F}_p)| = p + 1 - a_p$, where $a_p = \alpha_1 + \alpha_2$ is an integer in $[-2\sqrt{p}, 2\sqrt{p}]$. Given $a_p$, we have $(x - \alpha_1)(x - \alpha_2) = x^2 - a_p x + p$; the determinant here must be $p$ because Frobenius acts as multiplication by $p$ on $\Lambda^2 H^1_{\text{ét}}(A_{\overline{\mathbb{F}_q}}, \mathbb{Q}_\ell) = H^2_{\text{ét}}(A_{\overline{\mathbb{F}_q}}, \mathbb{Q}_\ell)$. The quadratic formula gives

$$\alpha_{1,2} = \frac{a_p \pm \sqrt{a_p^2 - 4p}}{2}. \tag{1}$$

Since $|a_p| \leq 2\sqrt{p}$, the square root is imaginary, so $|\alpha_1| = |\alpha_2| = p$, and the $\alpha_i$ are indeed Weil numbers. It is a consequence of our later discussion that for all primes $p$ and all integers

$a_p \in [-2\sqrt{p}, 2\sqrt{p}]$, there exists an elliptic curve over $\mathbb{F}_p$ with trace $a_p$. Tate's work implies that elliptic curves over finite fields are isogenous if and only if they have the same trace (equivalently, the same number of points), and these isogeny classes correspond to all of the Weil numbers above. Note in particular that the conjugacy class $\{\pm\sqrt{-p}\}$ corresponds to an isogeny class of supersingular elliptic curves.

We now consider the conjugacy class $\{\pm\sqrt{p}\}$, which is notably absent from the list above. These cannot arise from an elliptic curve, as the determinant of Frobenius would be $-p$ instead of $p$. So they must instead appear, each with multiplicity $g > 1$, as the Frobenius eigenvalues of an isogeny class of abelian varieties of dimension $g$. The determinant $(\sqrt{p})^g(-\sqrt{p})^g$ agrees with the desired $p^g$ if and only if $g$ is even. For $p \equiv 1 \pmod 4$, we will construct an explicit abelian variety of even dimension $\frac{p-1}{2}$ realizing $\pm\sqrt{p}$ as Frobenius eigenvalues:

**Proposition 2.** *Let $p \equiv 1 \pmod 4$, and let $C$ be the hyperelliptic curve $y^2 = x^p - x$, ramified over $\mathbb{P}^1_{\mathbb{F}_p}$ at all of its $\mathbb{F}_p$-points. The Jacobian $\mathrm{Jac}(C)$ has Frobenius eigenvalues $\pm\sqrt{p}$ with multiplicity $\frac{p-1}{2}$ each.*

Before proving this, we make a few observations. First, the quadratic twist of $C$ given by $y^2 = c(x^p - x)$ with $c \in \mathbb{F}_p^\times$ a non-square works as well, as we only need $\#C(\mathbb{F}_{p^2})$ below. Second, we do not claim that $\mathrm{Jac}(C)$ is simple; for now, we are only proving that it is isogenous to some power of a simple abelian variety whose isogeny class corresponds to $\{\pm\sqrt{p}\}$ under Honda-Tate. We also note that a similar construction cannot work for all primes; in fact, for $p = 2$ and $p = 3$, one can show by point counts similar to those below that no Jacobian of any curve has Frobenius eigenvalues $\pm\sqrt{p}$. For arbitrary $p \equiv 3 \pmod 4$, we note that $\frac{p-1}{2}$ is odd, and so cannot be the right dimension.

*Proof.* First, notice that since the ramification divisor of $C/\mathbb{P}^1$ has degree $p+1$, $C$ has genus $\frac{p-1}{2}$ by Riemann-Hurwitz. The Hasse-Weil bound then implies that

$$\#C(\mathbb{F}_{p^2}) \geq 1 + p^2 - 2gp = 1 + p. \tag{2}$$

We claim that our curve realizes this lower bound. If so, all of the Frobenius eigenvalues of $C$ must satisfy $\alpha_i^2 = p$; this forces half of them to be $\sqrt{p}$ and half $-\sqrt{p}$ in order for the Frobenius trace to be rational. Since $\mathrm{Jac}(C)$ has the same first cohomology as $C$, this would imply the proposition.

Our curve clearly has exactly $p+1$ $\mathbb{F}_p$-points, namely the point at infinity and the $p$ points $(x, 0)$. Now suppose $C$ has a point $(x_0, y_0) \in \mathbb{F}_{p^2} \times \mathbb{F}_{p^2}$ other than these. Then we must have $y_0 \neq 0$, as $g(x) = x^p - x$ has all its roots in $\mathbb{F}_p$. Let $\sigma : \mathbb{F}_{p^2} \to \mathbb{F}_{p^2}$ be the Frobenius map, so that $\sigma^2 = \mathrm{id}$. Then we have

$$\sigma(g(x_0)) = x_0^{p^2} - x_0^p \tag{3}$$

$$= x_0 - x_0^p = -g(x_0), \tag{4}$$

so $g(x_0)^{p-1} = -1$ since $g(x_0)$ is nonzero. But since $\frac{p+1}{2}$ is odd, we have

$$g(x_0)^{(p-1)(p+1)/2} = -1 \tag{5}$$

also, and so $g(x_0)$ is a non-square in $\mathbb{F}_{p^2}$. Thus all of the $\mathbb{F}_{p^2}$-points of $C$ are defined already over $\mathbb{F}_p$. □

# 1 The minimal dimension

Given a Weil $q$-number $\pi$, it is natural to ask for the dimension of the corresponding (isogeny class of) simple abelian varieties. This question is actually answered in Tate's work, conditional on the existence of such abelian varieties (later proved by Honda). It turns out that the Weil number determines $\mathrm{End}(A)\otimes\mathbb{Q}$, and this in turn determines the dimension. We will summarize how this all works, and defer to Tate for the proofs.

Fix a Weil $q$-number $\pi$. The rationalized endomorphism algebra $D = \mathrm{End}(A)\otimes\mathbb{Q}$ is a simple algebra with center $K = \mathbb{Q}(\pi)$, where $\pi$ corresponds to the relative Frobenius. As a central simple $K$-algebra, it can be specified by its class in

$$\mathrm{Br}(K) = \ker\left(\bigoplus_{v\nmid\infty}\mathbb{Q}/\mathbb{Z} \oplus \bigoplus_{v \text{ real}} \frac{1}{2}\mathbb{Z}/\mathbb{Z} \to \mathbb{Q}/\mathbb{Z}\right), \tag{6}$$

where the map is given by summing all entries. Tate showed that the Brauer invariants of $D$ are as follows: $\mathrm{inv}_v(D) = 0$ for $v \nmid p$ finite, $\frac{1}{2}$ for $v$ real, and

$$\mathrm{inv}_v(D) = \frac{\mathrm{ord}_v(\pi)}{\mathrm{ord}_v(q)} \cdot [K_v : \mathbb{Q}_p] = \mathrm{ord}_v(\pi) \cdot \frac{f_v}{\log_p(q)} \in \mathbb{Q}/\mathbb{Z} \tag{7}$$

for $v \mid p$, where $f_v$ is the inertia degree of the extension $K_v/\mathbb{Q}_p$.

Finally, the dimension of $A$ is given by $2\dim(A) = [D : K]^{1/2} \cdot [K : \mathbb{Q}]$. But $[D : K]$ is just the order of the Brauer class, which is the lcm of the orders of the above-mentioned elements of $\mathbb{Q}/\mathbb{Z}$. So $\dim A$ is easy to calculate in terms of the arithmetic of the field $K = \mathbb{Q}(\pi)$.

In the case where $q = p$ and $\pi = \pm\sqrt{p}$, $D$ is the algebra of Hamilton quaternions over $K = \mathbb{Q}(\sqrt{p})$, so $2\dim A = 2 \cdot 2$. So in fact the simple abelian varieties corresponding to $\pm\sqrt{p}$ are surfaces.

Indeed, we can construct such an abelian surface as the Weil restriction of an elliptic curve $E/\mathbb{F}_{p^2}$ with Frobenius eigenvalues $p, p$. Proof: $(\mathrm{Res}^{\mathbb{F}_{p^2}}_{\mathbb{F}_p} E)_{\mathbb{F}_p^2} = E \times E$ has Frobenius eigenvalues $p, p, p, p$, so the Frobenius eigenvalues of $\mathrm{Res}^{\mathbb{F}_{p^2}}_{\mathbb{F}_p} E$ must all be square roots of $p$, with rational sum.

Remark: Suppose $q = p$. Then for $v \mid p$, the second formula for $\mathrm{inv}_v(D)$ above clearly gives $0 \in \mathbb{Q}/\mathbb{Z}$. It follows that the Brauer class $[D]$ has order 2 if $K$ has a real place, and 1 otherwise. But $\pm\sqrt{p}$ are the only real Weil $p$-numbers, so for $\pi \neq \pm\sqrt{p}$ we have

$$2\dim A = [D : K]^{1/2} \cdot [K : \mathbb{Q}] = 2 \cdot [K : \mathbb{Q}]. \tag{8}$$

So over $\mathbb{F}_p$, our naive guess for $\dim A$ is correct in all cases except $\pi = \pm\sqrt{p}$.

## 2 Relation to our first construction

We have now constructed two abelian varieties over $\mathbb{F}_p$ with Frobenius eigenvalues $\pm\sqrt{p}$. By Tate's work, it follows that every isogeny summand of $\mathrm{Jac}(C)$ must be isogenous to $\mathrm{Res}_{\mathbb{F}_p}^{\mathbb{F}_{p^2}} E$, so in fact $\mathrm{Jac}(C) \sim (\mathrm{Res}_{\mathbb{F}_p}^{\mathbb{F}_{p^2}} E)^{(p-1)/4}$. Under the further hypothesis that $p \equiv 5 \pmod 8$, we can observe this fact directly.

We will construct one of the coordinate maps $\mathrm{Jac}(C) \to \mathrm{Res}_{\mathbb{F}_p}^{\mathbb{F}_{p^2}} E$; once we do this, the other coordinate maps should follow by composing with automorphisms of $C$. By the universal properties of the Weil restriction and the Jacobian, such maps are in bijection with maps $\mathrm{Jac}(C)_{\mathbb{F}_{p^2}} \to E$ over $\mathbb{F}_{p^2}$, and therefore with maps $C_{\mathbb{F}_{p^2}} \to E$ over $\mathbb{F}_{p^2}$. We will construct such a map (and indeed, such an $E$) as a quotient of $C_{\mathbb{F}_{p^2}}$ by a suitable group of automorphisms.

At this point, the entire problem is over $\mathbb{F}_{p^2}$, so we abusively write $C$ for $C_{\mathbb{F}_{p^2}}$ and work in the category of $\mathbb{F}_{p^2}$-schemes unless otherwise specified.

Before studying the automorphisms of $C$, let's see what properties are forced upon it by Riemann-Hurwitz.[1] If $G$ is a subgroup of $\mathrm{Aut}(C)$ of order $n$, Riemann-Hurwitz says that

$$p - 3 = 2g_C - 2 = n(2g_{C/G} - 2) + \deg R = \deg R, \tag{9}$$

where $R$ is the ramification divisor of $\pi : C \to C/G$. The degree of $R$ can be calculated after passing to an algebraic closure: it is

$$\begin{aligned}
\deg R &= \sum_{x \in (C/G)(\overline{\mathbb{F}_{p^2}})} n - |\pi^{-1}(x)| &(10)\\
&= \sum_{y \in C(\overline{\mathbb{F}_{p^2}})} |\operatorname{Stab}_G(y)| - 1 &(11)\\
&= \sum_{1 \neq g \in G} |(C_{\overline{\mathbb{F}_{p^2}}})^g|; &(12)
\end{aligned}$$

that is, the sum of the geometric fix loci of the non-identity elements of $G$. So given that the quotient map is generically separable, it is necessary and sufficient for this quantity to equal $p - 3$.

Now we look into the structure of $\mathrm{Aut}(C)$. Since $C$ is a hyperelliptic curve branched at all $p + 1$ $\mathbb{F}_p$-points of $\mathbb{P}^1$, it follows that any automorphism $\varphi : C \to C$ fits into a commutative square

$$\begin{tikzcd}
C \arrow[r, "\varphi"] \arrow[d, "\pi"'] & C \arrow[d, "\pi"] \\
\mathbb{P}^1 \arrow[r, "\overline{\varphi}"] & \mathbb{P}^1,
\end{tikzcd}$$

[1] The map we eventually construct will have degree prime to $p$, so it will be generically separable.

where $\overline{\varphi}$ is an automorphism of $\mathbb{P}^1$ preserving the $\mathbb{F}_p$-points. Such an automorphism is given by a fractional linear transformation $x \mapsto \frac{ax+b}{cx+d}$ with $a, b, c, d \in \mathbb{F}_p$, modulo scalars. Conversely, for any given $\overline{\varphi} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, one can calculate that there are exactly two $\varphi \in \mathrm{Aut}(C)$ inducing it, given by the formula

$$(x, y) \mapsto \left( \frac{ax+b}{cx+d}, \frac{\sqrt{\det} \cdot y}{(cx+d)^{(p+1)/2}} \right), \tag{13}$$

where $\sqrt{\det} \in \mathbb{F}_{p^2}$ is one of the two square roots of $ad - bc \in \mathbb{F}_p^\times$. In the case $\overline{\varphi} = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$, the identity automorphism is the one with $\sqrt{\det} = a^{(p+1)/2}$; that is, $\sqrt{\det} = a$ if $a \in (\mathbb{F}_p^\times)^2$ and $-a$ otherwise.

The result of this discussion is the following description of $\mathrm{Aut}(C)$: it is the group of invertible $2 \times 2$ matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ over $\mathbb{F}_p$ equipped with $\sqrt{\det} \in \mathbb{F}_p^2$, with coordinate-wise multiplication, modulo the subgroup of elements

$$\left( \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}, a^{(p+1)/2} \right). \tag{14}$$

Observe that this fits into a non-split short exact sequence

$$1 \to \pm 1 \to \mathrm{Aut}(C) \to \mathrm{PGL}_2(\mathbb{F}_p) \to 1, \tag{15}$$

where $-1 := (I, -1)$ represents the hyperelliptic involution $(x, y) \mapsto (x, -y)$.

So far we have not used the condition that $p \equiv 5 \pmod 8$. For such $p$, we now construct a subgroup $G < \mathrm{Aut}(C)$ with order $\frac{p-1}{2}$ such that each non-identity element fixes exactly two geometric points, resulting in the sum of $p - 3$ required by Riemann-Hurwitz. Let $H$ denote the maximal prime-to-2 subgroup of $\mathbb{F}_p^\times$, namely $H = (\mathbb{F}_p^\times)^4$. Fix a non-square $\alpha \in \mathbb{F}_p^\times$, along with a choice of square root $\sqrt{\alpha} \in \mathbb{F}_{p^2}^\times$. Then the involution

$$\left( \begin{pmatrix} 0 & -\alpha \\ 1 & 0 \end{pmatrix}, \sqrt{\alpha} \right) \tag{16}$$

normalizes the subgroup

$$\left\{ \left( \begin{pmatrix} \beta^2 & 0 \\ 0 & 1 \end{pmatrix}, \beta \right) : \beta \in H \right\} \tag{17}$$

and we define $G$ to be the semidirect product. This is a dihedral group of order $2(\frac{p-1}{4})$, and one can calculate directly that it has the desired properties.[2]

[2] For $\left( \begin{pmatrix} 0 & -\alpha \\ 1 & 0 \end{pmatrix}, \sqrt{\alpha} \right)$, note that there are two fixed points $x = \pm\sqrt{-a}$ after projecting to $\mathbb{P}^1$. The preimages in $C$ of one of these points are both fixed, and those of the other are transposed.

Remark: if $p \equiv 1 \pmod 8$, it is not clear how to make this construction work. It may even be impossible, since there is no a priori reason that the map $C \to E$ must be Galois. The problem is that the hyperelliptic involution $-1 \in \mathrm{Aut}(C)$ has $p+1 > p-3$ geometric fixed points by itself, and so it cannot lie in $G$. The natural analogue of (17) above would be a cyclic subgroup of order $\frac{p-1}{4}$, which is even for $p \equiv 1 \pmod 8$. Therefore this subgroup would contain $-1$.