RATIONALITY FOR ABELIAN VARIETIES OVER FINITE FIELDS

NIR ELBER

Abstract. We prove the rationality piece of the Weil conjectures for abelian varieties, and we prove the full Weil conjectures for elliptic curves. The proof essentially arises out of an understanding of the characteristic polynomial of an endomorphism, in particular of the Frobenius endomorphism.

Contents

1. Introduction

The goal of this paper is to prove the rationality piece of the Weil conjectures for abelian varieties. As such, we begin by stating the Weil conjectures [Wei49]; our exposition here borrows from [Ras07]. Let X be a projective variety over a finite field $\mathbb{F}_q$. The main character of the Weil conjectures is the following zeta function.

Definition 1.1 (Z-function)**.** *Let X be a projective variety over a finite field $\mathbb{F}_q$. Then we define the Z-function as a formal power series*

$$Z(X,t) \coloneqq \exp\left(\sum_{m=1}^{\infty} \#X\left(\mathbb{F}_{q^m}\right)\frac{t^m}{m}\right) \in \mathbb{Q}\left[\!\left[t\right]\!\right]. \tag{1.1}$$

Remark 1.2. *In analogy with the Riemann ζ-function*

$$\zeta(s) = \prod_{p \text{ prime}} \frac{1}{1-p^{-s}} = \prod_{\text{closed } \mathfrak{p}\in \operatorname{Spec}\mathbb{Z}} \frac{1}{1-\#k(\mathfrak{p})^{-s}},$$

one can show that

$$Z\left(X, q^{-s}\right) = \prod_{\text{closed } x\in X} \frac{1}{1-\#k(x)^{-s}}.$$

The proof is not hard, but we will not need this, so we will not show it here; see [Ras07, Proposition 1.5].

Roughly speaking, $Z(X,t)$ is a gadget which stores information about the number of $\mathbb{F}_{q^m}$-points in X; the Weil conjectures establish strong properties of $Z(X,t)$ and hence on these point-counts.

Date: 5 May 2023.

Theorem 1.3. *Let X be a projective variety over a finite field $\mathbb{F}_q$ of dimension d.*

(1) Rationality: $Z(X,t)$ can be written as

$$Z(X,t) = \frac{P_1(t)P_3(t)\cdots P_{2d-1}(t)}{P_0(t)P_1(t)\cdots P_{2d}(t)},$$

where $P_j \in \mathbb{Z}[t]$ is a polynomial.

(2) Functional equation: we have

$$Z\left(X, q^{-d}t^{-1}\right) = \pm q^{de/2}t^e Z(X,t)$$

as formal power series, where e is the Euler characteristic of X.

(3) Riemann hypothesis: the roots of the polynomial P_j have magnitude $q^{-j/2}$, for each j. Further, $P_0(t) = 1 - t$ and $P_{2d}(t) = 1 - q^d t$.

We will not get close to fully proving Theorem 1.3. Instead, the main goal of this paper is to prove rationality for abelian varieties.

Theorem 1.4 (Rationality)**.** *Let A be an abelian variety over a finite field $\mathbb{F}_q$ of dimension d. Then one has*

$$Z(A,t) = \frac{P_1(t)P_3(t)\cdots P_{2d-1}(t)}{P_0(t)P_2(t)\cdots P_{2d}(t)}$$

where each $P_j(t)$ is a polynomial with integer coefficients, depending on the eigenvalues of the Frobenius $\pi_A \colon A \to A$.

The Frobenius morphism $\pi_A \colon A \to A$ of an abelian variety over a finite field will be defined in Definition 3.1, and its eigenvalues are its eigenvalues as an operator on $V_\ell A$ for (any) prime ℓ coprime to q.

1.1. **Layout.** In section 2, we define and prove basic properties about the characteristic polynomial of an endomorphism of an abelian variety. Most notable is that this characteristic polynomial agrees no matter which Tate module one chooses, which is shown in Proposition 2.14. Then we use this built theory to prove Theorem 1.4 in section 3; the main input here is an understanding of how the Frobenius morphism enables point-counting, shown in Proposition 3.6.

Throughout, we use elliptic curves as our examples, and we dedicate section 4 to them. Most notably, we are able to complete the proof of the Weil conjectures in this case in Theorems 4.2 and 4.3, and we go on to use this machinery to actually count points in section 4.2.

1.2. **Notation.** Throughout, k is a field. We let $\mathrm{Hom}_k(A,B)$ denote the set of homomorphisms of abelian k-varieties $A \to B$, and set $\mathrm{End}_k(A) \coloneqq \mathrm{Hom}_k(A,A)$ and $\mathrm{End}_k^0(A) \coloneqq \mathrm{End}_k(A) \otimes_{\mathbb{Z}} \mathbb{Q}$; notably, $\mathrm{End}_k(A)$ is a free $\mathbb{Z}$-module of finite rank by [Elb22, Corollary 3.6]. We repress the subscript k when no confusion will arise. Given a prime ℓ not divisible by $\operatorname{char} k$, we define the ℓ-adic Tate module $T_\ell A$ as the inverse limit of the ℓ-torsion modules $A\left[\ell^\bullet\right]$, and we set $V_\ell A \coloneqq T_\ell A \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$.

For this paper, particularly relevant are the characteristic polynomial of an endomorphism φ which will be denoted P_φ and the Frobenius endomorphism of an abelian variety A over a finite field which will be denoted π_A.

Remark 1.5. *Throughout this paper, we freely assume any theory about abelian varieties as established in [Elb22].*

2. The Characteristic Polynomial

In this section, we define the characteristic polynomial and establish its basic facts. Our exposition closely follows [Mil08, Section I.10]. Throughout, A is an abelian k-variety, and $\varphi \colon A \to A$ is an endomorphism. We also take a moment to establish the following example [Elb22, Example 2.1] which will pop up a few times throughout the paper.

Example 2.1. *Let k be a field with $\operatorname{char} k \neq 3$. Then $E \coloneqq \operatorname{Proj} k[X,Y,Z]/\left(Y^2Z - X^3 - Z^3\right)$ is an elliptic curve. Indeed, this is the elliptic curve cut out in the plane by $y^2 = x^3 + 1$, which we see does make an elliptic curve because it is smooth: the discriminant here is 3^3, which is not 0 because $\operatorname{char} k \neq 3$.*

2.1. **The Definition.** It will be beneficial for us to understand the characteristic polynomial of an endomorphism $\varphi\colon A \to A$. For any prime ℓ not divisible by $\operatorname{char} k$, the endomorphism φ induces a map $V_\ell\varphi\colon V_\ell A \to V_\ell A$, so it is tempting to define the characteristic polynomial as arising from these representations as

$$P_\varphi(r) \stackrel{?}{=} \det(\varphi - r \mid V_\ell A).$$

However, it is not clear that this definition is independent of ℓ, or even that it has rational coefficients. We will be able to show these things, but not yet.

For our definition, we would like to define the characteristic polynomial based on data internal to φ. As motivation, we have the following remark.

Remark 2.2. *Suppose our abelian variety is $A = \mathbb{C}^d/\Lambda$ for some lattice Λ. Then we want the characteristic polynomial of φ to arise from its action on $H_1(A, \mathbb{Q}) \cong \Lambda \otimes_{\mathbb{Z}} \mathbb{Q}$, which is the characteristic-0 analogue of $V_\ell A$. We're in characteristic 0, so there are no separability concerns, so we can compute that we want*

$$|P_\varphi(n)| = |\det(\varphi - [n] \mid H_1(A, \mathbb{Q}))| \stackrel{*}{=} \#\left(\frac{\Lambda}{(\varphi - [n])\Lambda}\right) = \#\left(\frac{(\varphi - n)^{-1}\Lambda}{\Lambda}\right) = \#\ker(\varphi - [n]) = \deg(\varphi - [n])$$

whenever $\varphi \neq [n]$. Here, $\stackrel{*}{=}$ is a general fact about lattices which follows from row-reducing the vector-space isomorphism $(\varphi - [n])\colon (\Lambda \otimes_{\mathbb{Z}} \mathbb{Q}) \to (\Lambda \otimes_{\mathbb{Z}} \mathbb{Q})$.

The point is that we will want to define $P_\varphi([n])$ as $\deg(\varphi - [n])$ for all integers n; notably, we can amend the situation of $\varphi = n$ by simply defining $\deg\varphi \coloneqq 0$ when φ fails to be an isogeny. However, from this definition, it is now not obvious that there exists a polynomial P_φ which will interpolate the function $n \mapsto \deg(\varphi - [n])$, so this is our next task. For clarity, we will work in slight generality for the following results.

Lemma 2.3. *Fix an abelian k-variety A. For any endomorphisms $\alpha, \beta \in \operatorname{End}(A)$, the $\mathbb{Z} \to \mathbb{Z}$ function $n \mapsto \deg(n\alpha + \beta)$ can be interpolated by a unique polynomial $P_{\alpha,\beta}$ with rational coefficients and degree at most $2\dim A$. If α is an isogeny, then $P_{\alpha,\beta}$ has degree $2\dim A$ and leading coefficient $\deg\alpha$.*

Proof. The uniqueness of $P_{\alpha,\beta}$ holds because $\mathbb{Z}$ is an infinite set: namely, any two polynomials interpolating the given points will have a difference equal to a polynomial with infinite roots, so the difference will vanish. As such, the concern is existence. Anyway, the main content of the proof requires intersection theory, which we will not bother to properly introduce here. For brevity, set $d \coloneqq \dim A$.

Fix some symmetric very ample divisor D on A (i.e., we require $[-1]^*D = D$), and for brevity, set $D_n \coloneqq (n\alpha + \beta)^*D$. Flat pullback of the intersection product yields

$$\deg(n\alpha + \beta) \cdot \underbrace{(D, \dots, D)}_{d} = \underbrace{(D_n, \dots, D_n)}_{d},$$

so we would like to know that $n \mapsto (D_n, \dots, D_n)$ can be interpolated by a polynomial in n. Well, to compute D_n, we note that [Elb22, Corollary 2.13] implies

$$(n\alpha + \beta + \alpha + \alpha)^*D + (n\alpha + \beta)^*D + \alpha^*D + \alpha^*D = (n\alpha + \beta + \alpha)^*D + (n\alpha + \beta + \alpha)^*D + (2\alpha)^*D,$$

so

$$D_{n+2} - 2D_{n+1} + D_n = -2\alpha^*D + (2\alpha)^*D.$$

Because D is symmetric, [Elb22, Corollary 2.14] implies $-2\alpha^*D + (2\alpha)^*D = 2\alpha^*D$. Now, we claim that

$$D_n \stackrel{?}{=} n(n-1)\alpha^*D + nD_1 - (n-1)D_0 \tag{2.1}$$

for any $n \in \mathbb{Z}$. Indeed, we set $E_n \coloneqq D_n - n(n-1)\alpha^*D - nD_1 + (n-1)D_0$ so that

$$E_{n+2} - 2E_{n+1} + E_n = 0.$$

Thus, computing $E_0 = 0$ and $E_1 = 0$, we see that $E_n = 0$ for all $n \in \mathbb{Z}$, from which (2.1) follows.

We are now essentially done. Expanding $(D_n, \dots, D_n)$ linearly shows that $n \mapsto (D_n, \dots, D_n)$ is interpolated by a monic polynomial of degree $2d$, where the leading term is given by

$$\frac{(n(n-1)\alpha^*D, \dots, n(n-1)\alpha^*D)}{(D, \dots, D)} = n(n-1)^d \cdot \frac{(\alpha^*D, \dots, \alpha^*D)}{(d, \dots, D)} = (n(n-1))^d \deg\alpha,$$

as predicted. ∎

We now extend our interpolation from integers to rational numbers. Quickly, recall that $\deg \varphi = 0$ if $\varphi \in \operatorname{End}(A)$ fails to be an isogeny. We note that

$$\deg(n\varphi) = \deg([n]) \deg \varphi = n^{2 \dim A} \deg \varphi,$$

so for any $q \in \mathbb{Q}$ and $\varphi \in \operatorname{End}(A)$, we may define $\deg(q\varphi) \coloneqq q^{2 \dim A} \deg \varphi$.

Proposition 2.4. *Fix an abelian k-variety A. For $\alpha, \beta \in \operatorname{End}^0(A)$, there is a unique polynomial $P_{\alpha,\beta} \in \mathbb{Q}[t]$ of degree at most $2 \dim A$ such that*

$$P_{\alpha,\beta}(q) = \deg(q\alpha + \beta).$$

Further, if α is an isogeny, then $P_{\alpha,\beta}$ has degree $2 \dim A$ and leading coefficient $\deg \alpha$.

Proof. The proof of uniqueness is the same as Lemma 2.3, so the concern is existence. For brevity, set $d \coloneqq \dim A$.

To begin $\alpha, \beta \in \operatorname{End}^0(A)$ has some N such that $N\alpha, N\beta \in \operatorname{End}^0(A)$, so Lemma 2.3 produces us a polynomial $P_{N\alpha,N\beta}$ interpolating $n \mapsto \deg(nN\alpha + N\beta)$. We claim that the needed polynomial is $N^{-2d} P_{N\alpha,N\beta}$. Well, for any $\frac{r}{s} \in \mathbb{Q}$ with $r, s \in \mathbb{Z}$, we would like to compute $N^{-2d} P_{N\alpha,N\beta}(r/s)$. For this, we note that

$$s^{-2d} P_{N\alpha,Ns\beta}(sn) = s^{-2d} \deg(nNs\alpha + Ns\beta) = \deg(nN\alpha + N\beta) = P_{N\alpha,N\beta}(n)$$

for any $n \in \mathbb{Z}$, by construction and the degree of $[s]$, so it follows that $s^{-2d} P_{N\alpha,Ns\beta}(st) = P_{N\alpha,N\beta}(t)$ as polynomials. In particular, plugging in $x = r/s$, we see that

$$N^{-2d} P_{N\alpha,N\beta}(r/s) = N^{-2d} s^{-2d} P_{N\alpha,Ns\beta}(r) = N^{-2d} s^{-2d} \deg(rN\alpha + Ns\beta) = \deg\left(\frac{r}{s}\alpha + \beta\right),$$

where the last equality is by how deg is defined on $\operatorname{End}^0(A)$. This is what we wanted. ∎

At long last, here is our definition.

Definition 2.5 (characteristic polynomial)**.** *Fix an abelian k-variety. For any endomorphism $\varphi \in \operatorname{End}^0(A)$, we let $P_\varphi(x) \in \mathbb{Q}[t]$ be the unique monic polynomial of degree $2 \dim A$ interpolating $P_\varphi(q) = \deg(\varphi - q[1])$. This polynomial exists and is unique by Proposition 2.4.*

Remark 2.6. *We have not shown that P_φ has integer coefficients in the case when $\varphi \in \operatorname{End}(A)$. This is in fact true, but it is not obvious from the argument we gave above; namely, Lemma 2.3 will only tell us that the polynomial has bounded denominator. Nonetheless, we will be able to show that P_φ has integer coefficients much later in Corollary 2.15.*

Example 2.7. *Fix an abelian k-variety. Setting $\varphi \coloneqq [r]$ for some $r \in \mathbb{Z}$, we see*

$$P_{[r]}(n) = \deg([r] - [n]) = \deg([r - n]) = (r - n)^{2 \dim A},$$

so $P_{[r]}(t) = (t - r)^{2 \dim A}$, which does indeed have the required properties.

Example 2.8. *Work in the context of Example 2.1, and suppose $\operatorname{char} k = 0$, and suppose $\zeta_3 \in k$. Define $\varphi \colon E \to E$ by $\varphi([X : Y : Z]) \coloneqq [\zeta_3 X : Y : Z]$, which is a scheme morphism fixing $0_E = [0 : 1 : 0]$ and thus an endomorphism. Lemma 2.3 implies that $n \mapsto \deg(\varphi - [n])$ can be interpolated by our monic quadratic polynomial P_φ.*

- *Because φ is an automorphism (φ^3 is the identity), $P_\varphi(0) = \deg \varphi = 1$.*
- *Because everything possible is separable, $P_\varphi(1) = \deg(\varphi - [1])$ is $\#\ker(\varphi - [1])(\overline{k})$, so we want to count $[X : Y : Z] \in E(\mathbb{C})$ such that $\varphi([X : Y : Z]) = [X : Y : Z]$. This is equivalent to $X = 0$, so we have either $[0 : 1 : 0]$ or $[0 : \pm 1 : 1]$, so $P_\varphi(1) = 3$ follows.*

Interpolating the above points, we conclude $P_\varphi(x) = x^2 + x + 1$. This is indeed monic with integer coefficients.

2.2. **Degree Is Polynomial.** Because it is not so much more work, we might as well upgrade Proposition 2.4 to show that $\deg \colon \operatorname{End}^0(A) \to \mathbb{Q}$ is essentially a polynomial. One must be a little careful with this, so here is our definition.

Definition 2.9 (polynomial function)**.** *Fix a k-vector space V. A map $f \colon V \to k$ is a polynomial if and only if, for any linearly independent set of vectors $\{v_1, \dots, v_n\} \subseteq V$, there exists a polynomial $P \in k[x_1, \dots, x_n]$ such that*

$$f(c_1 v_1 + \cdots + c_n v_n) = P(c_1, \dots, c_n)$$

for any scalars $c_1, \dots, c_n \in k$. If P has some property (such as being homogeneous, having bounded total degree, or bounded degree in any variable), we apply the same descriptor to f.

Here is a quick way to check that we have a polynomial function.

Lemma 2.10. *Fix a vector space V over an infinite field k. Given a function $f\colon V \to k$, suppose there exists a nonnegative integer d such that $c \mapsto f(cv+w)$ is a polynomial function $k \to k$ of degree at most d, for any $v, w \in V$. Then f is a polynomial function of degree at most d in any variable.*

Proof. By inducting on n, we claim that any finite set $\{v_1, \dots, v_n, w\}$ makes the function

$$(x_1, \dots, x_n) \mapsto f(x_1v_1 + \cdots + x_nv_n + w)$$

a polynomial function of degree at most d in any variable. At $n = 0$, this is a constant function, so there is nothing to say. For the inductive step, we view $(x_1, \dots, x_{n+1}) \mapsto f(x_1v_1 + \cdots + x_nv_n + x_{n+1}v_{n+1} + w)$ as a function in x_{n+1} so that the hypothesis implies that it is a polynomial function

$$f(x_1v_1 + \cdots + x_nv_n + x_{n+1}v_{n+1} + w) = \sum_{i=0}^{d} a_i(x_0, \dots, x_n)x_{n+1}^i$$

of degree at most d, where the coefficients a_i are just some function $k^n \to k$.

It remains to show that the coefficients $a_i(x_0, \dots, x_n)$ are themselves polynomials of degree at most d in any variable. Well, choose $n+1$ distinct scalars $c_0, \dots, c_{n+1} \in k$ to yield the equations

$$f(x_1v_1 + \cdots + x_nv_n + c_jv_{n+1} + w) = \sum_{i=0}^{d} a_i(x_0, \dots, x_n)x_j^i$$

for any c_j. We may now use Cramér's rule in order to solve for the coefficients $a_i(x_0, \dots, x_n)$ in terms of the polynomial functions $(x_1, \dots, x_n) \mapsto f(x_1v_1 + \cdots + x_nc_n + c_jv_{n+1} + w)$; note that this application of Cramér's rule is legitimate because the matrix $\left\{c_j^i\right\}_{0 \le i,j \le d}$ has nonzero determinant by the Vandermonde determinant—here we have used that the c_j are distinct. Thus, the $a_i(x_0, \dots, x_n)$ are (linear combinations of) polynomials of degree at most d in any variable, so the result follows. ∎

Thus, Proposition 2.4 immediately produces the following result.

Proposition 2.11. *Fix an abelian k-variety A. Then* $\deg\colon \mathrm{End}^0(A) \to \mathbb{Q}$ *is a homogeneous polynomial function of degree* $2 \dim A$.

Proof. We have a polynomial function by combining Lemma 2.10 with Proposition 2.4. Thus, fixing a basis $\{\varphi_0, \dots, \varphi_n\}$ of $\mathrm{End}^0(A)$, we get a polynomial $P \in \mathbb{Q}[x_1, \dots, x_n]$ such that

$$\deg(c_1\varphi_1 + \cdots + c_n\varphi_n) = P(c_1, \dots, c_n).$$

Because $\mathbb{Q}$ is an infinite field, this polynomial P is unique: indeed, if P and Q are polynomials both satisfying the above, then $P - Q$ vanishes on $\mathbb{Q}^n$, so it must vanish. For example, for fixed $(c_1, \dots, c_{n-1}) \in \mathbb{Q}^{n-1}$, the function $P(c_1, \dots, c_{n-1}, x) - Q(c_1, \dots, c_{n-1}, x)$ is a polynomial with infinite roots and thus must vanish; this allows us to induct downwards to achieve $P = Q$.

We must still show that P is a homogeneous polynomial of degree $2d \coloneqq 2 \dim A$. In other words, we would like to show that $P(\lambda x_1, \dots, \lambda x_n) = \lambda^{2d} P(x_1, \dots, x_n)$ for any $\lambda \in \mathbb{Q}$. For $\lambda = 0$, there is nothing to say. Otherwise, we note that

$$\lambda^{-2d} P(\lambda c_1, \dots, \lambda c_n) = \lambda^{-2d} \deg(\lambda c_1\varphi_1 + \cdots + \lambda c_n\varphi_n) = \deg(c_1\varphi_1 + \cdots + c_n\varphi_n) = P(c_1, \dots, c_n)$$

for any $(c_1, \dots, c_n) \in \mathbb{Q}^n$. The uniqueness of the polynomial P establishes the conclusion. ∎

2.3. **Coherence with Tate Modules.** We advertized at the start that P_φ that should be the characteristic polynomial of φ acting on the $\mathbb{Q}_\ell$-vector space $V_\ell A$. In this subsection, we show this, but we warn that the argument is somewhat technical. The following lemma explains how we will show that our two polynomials are the same.

Lemma 2.12. *Fix monic polynomials $P, Q \in \mathbb{Q}_\ell[t]$ of the same degree, and factor them as $\overline{\mathbb{Q}_\ell}[t]$ as $P(t) = \prod_{i=1}^N (t - \alpha_i)$ and $Q(t) = \prod_{i=1}^N (t - \beta_i)$. If*

$$\left| \prod_{i=1}^N F(\alpha_i) \right|_\ell = \left| \prod_{i=1}^N F(\beta_i) \right|_\ell$$

for any $F \in \mathbb{Z}[t]$, then $P = Q$.

Proof. We make two quick reductions.

- We may actually choose any $F \in \mathbb{Q}[t]$. Indeed, by clearing denominators, we may find $d \in \mathbb{Z}$ so that $(dF) \in \mathbb{Z}[t]$, from which we calculate
$$\left| \prod_{i=1}^N F(\alpha_i) \right|_\ell = |d|_\ell^{-N} \left| \prod_{i=1}^N (dF)(\alpha_i) \right|_\ell = |d|_\ell^{-N} \left| \prod_{i=1}^N (dF)(\beta_i) \right|_\ell = \left| \prod_{i=1}^N F(\beta_i) \right|_\ell.$$
- Continuity allows us to choose $F \in \mathbb{Q}_\ell[t]$. Notably, the function $\mathbb{Q}_\ell^n \to \mathbb{R}$ defined by
$$(c_1, \dots, c_n) \mapsto \left| \prod_{i=1}^N \left(\sum_{j=0}^n c_j \alpha_i^j \right) \right|_\ell - \left| \prod_{i=1}^N \left(\sum_{j=0}^n c_j \alpha_i^j \right) \right|_\ell$$
is continuous and vanishes on the dense subset $\mathbb{Q}^n \subseteq \mathbb{Q}_\ell^n$, so it will vanish on all of $\mathbb{Q}_\ell^n$.

Fix some $\gamma \in \overline{\mathbb{Q}_\ell}$, and let d and e be the order of vanishing of P and Q at γ, respectively. Because P and Q are monic and have the same degree, it is enough to show that $d = e$ as γ ranges over $\overline{\mathbb{Q}_\ell}$.

The idea, now, is to let F be the monic minimal polynomial for some $\gamma' \in \mathbb{Q}_\ell(\gamma)$ which is "close" to γ; notably, $\mathbb{Q}_\ell(\gamma)$ is a finite extension of $\mathbb{Q}_\ell$ and thus complete. To use the hypothesis efficiently, we let $H \subseteq \mathrm{Gal}(\overline{\mathbb{Q}_\ell}/\mathbb{Q}_\ell)$ denote a subset such that $\{\sigma(\gamma) : \sigma \in H\}$ is the set of Galois conjugates of γ. Thus, we compute

$$\left| \prod_{i=1}^N F(\alpha_i) \right| = \left| \prod_{i=1}^N \left(\prod_{\sigma \in H} (\alpha_i - \sigma(\gamma')) \right) \right|_\ell = \prod_{\sigma \in H} \prod_{i=1}^N |\alpha_i - \sigma(\gamma')|.$$

Now, P has coefficients in $\mathbb{Q}_\ell$, so $\sigma P = P$ for any $\sigma \in H$, so σ merely permutes the roots α_i. As such, we find

$$\left| \prod_{i=1}^N F(\alpha_i) \right| = \prod_{\sigma \in H} \left(\prod_{i=1}^N |\sigma(\alpha_i) - \sigma(\gamma')|_\ell \right) = \prod_{\sigma \in H} \left(\prod_{i=1}^N |\alpha_i - \gamma'|_\ell \right),$$

where the last equality holds because automorphisms σ do not adjust $|\cdot|_\ell$. Taking roots and applying the hypothesis, we conclude

$$\prod_{i=1}^N |\gamma' - \alpha_i|_\ell = \prod_{i=1}^N |\gamma' - \beta_i|_\ell$$

for any $\gamma' \in \mathbb{Q}_\ell(\gamma)$. Thus, supposing without loss of generality that $d \geq e$, we see

$$1 = \lim_{\gamma' \to \gamma} \left(|\gamma - \gamma'|^{d-e} \cdot \prod_{\substack{1 \leq i \leq N \\ \alpha_i \neq \gamma}} |\alpha_i - \gamma'| \cdot \prod_{\substack{1 \leq i \leq N \\ \beta_i \neq \gamma}} |\beta_i - \gamma'| \right),$$

so $d = e$ is follows. ∎

The condition in Lemma 2.12 might look annoying to interface with, but it will come from the following lemma. Most notably, we will plug in $E = \mathrm{End}^0(A)$ and $k = \mathbb{Q}$ and $d = \deg$ in the sequel.

Lemma 2.13. *Let E be a finite-dimensional algebra over an infinite field k. Suppose that $d \colon E \to k$ is a polynomial function such that $d(\alpha\beta) = d(\alpha)d(\beta)$ for any $a, b \in E$. Given $\varphi \in E$, suppose $P_\alpha(t)$ is a monic polynomial interpolating $c \mapsto d(\varphi - c)$. Factoring $P_\varphi(t) = \prod_{i=1}^N (t - \alpha_i)$, we have*

$$d(F(\alpha)) = d(c)(-1)^{N \deg F} \prod_{i=1}^N F(\alpha_i)$$

for any $F \in K[t]$ with leading coefficient c.

Proof. The point is to extend k to include the roots of F and the roots of P_φ. Indeed, let ℓ be some finite extension of k containing these roots. Then $E_\ell \coloneqq E \otimes_k \ell$ is also a finite-dimensional ℓ-algebra: letting $\{\gamma_1, \dots, \gamma_n\}$ denote a basis of E as a k-vector space, these elements remain a basis of E_ℓ as an ℓ-vector space. On E, there is a polynomial $P \in k[t_1, \dots, t_n]$ such that

$$d(c_1\gamma_1 + \cdots + c_n\gamma_n) = P(\gamma_1, \dots, \gamma_n)$$

for any $(c_1, \dots, c_n) \in k^n$. Thus, we define d_ℓ by this same polynomial P to be a polynomial function $E_\ell \to \ell$. We are given that $d(\alpha\beta) = d(\alpha)d(\beta)$ for any $\alpha, \beta \in E$, so we see that

$$d_\ell(c_1\gamma_1 + \cdots + c_n\gamma_n)d_\ell(d_1\gamma_1 + \cdots + d_n\gamma_n) - d_\ell((c_1\gamma_1 + \cdots + c_n\gamma_n)(d_1\gamma_1 + \cdots + d_n\gamma_n))$$

is some large polynomial function $\ell^{2n} \to \ell$ vanishing on k^{2n}, so it must vanish as a polynomial (because k is an infinite field), so we retain $d_\ell(\alpha\beta) = d_\ell(\alpha)d_\ell(\beta)$ for any $\alpha, \beta \in E_\ell$.

The rest of the proof is computation. If $F = 0$, there is noting to say; otherwise, factor the polynomial F as $F(t) = c\prod_{j=1}^d (t - \beta_j)$ with $c \neq 0$, so we compute

$$d(F(\alpha)/c) = d_\ell\left(\prod_{j=1}^d (\alpha - \beta_j)\right) = \prod_{j=1}^d d_\ell(\alpha - \beta_j) = \prod_{j=1}^d P_\varphi(\beta_j) = \prod_{j=1}^d \prod_{i=1}^N (\beta_j - \alpha_i) = (-1)^{dN} \prod_{i=1}^N F(\alpha_i),$$

finishing. ∎

And here is our result.

Proposition 2.14. *Fix an abelian k-variety A, and fix an endomorphism $\varphi \in \operatorname{End}(A)$. For any prime ℓ not divisible by* $\operatorname{char} k$*, the characteristic polynomial P_φ agrees with the characteristic polynomial of $V_\ell\varphi \colon V_\ell A \to V_\ell A$.*

Proof. The main point is to show that

$$|\deg \varphi|_\ell = |\det V_\ell\varphi|_\ell \tag{2.2}$$

for any endomorphism $\varphi \in \operatorname{End}(A)$. We proceed in steps.

(1) If φ fails to be an isogeny, then $\deg \varphi = 0$ by definition, and we claim $\det V_\ell\varphi = 0$ as well. Indeed, note $\ker \varphi$ is an abelian group scheme of positive dimension, and upon taking the connected component $B \subseteq \ker \varphi$ of $0_A \in \ker \varphi$, we see that B is an abelian subvariety of positive dimension. Then $V_\ell B \subseteq V_\ell A$ lives in the kernel of $T_\ell\varphi$ and has positive dimension, so $\det V_\ell\varphi = 0$ follows.

(2) Suppose $\varphi \colon A \to A$ is a purely inseparable isogeny. In this case, we must have $p \coloneqq \operatorname{char} k > 0$. Here, $d \coloneqq \deg \varphi$ is the degree of a purely inseparable field extension and hence must be a power of p, so $|\deg \varphi|_\ell = 1$ follows.

On the other hand, it is a fact that $\ker \varphi$ is a p-group. Note that this is not entirely obvious due to inseparability, and we will not show it here, instead referencing to [EGM, Exercise 4.4].[1] The point is that φ has no ℓ-power-torsion, so $\varphi \colon A[\ell^\nu] \to A[\ell^\nu]$ is always an isomorphism, so $T_\ell\varphi \colon T_\ell A \to T_\ell A$ is an isomorphism. As such, the determinant of the map $V_\ell[d]$ had better live in $\mathbb{Z}_\ell^\times$ (because $V_\ell[d]$ arises from an isomorphism of $\mathbb{Z}_\ell$-modules), yielding $|\deg V_\ell\varphi|_\ell = 1$ as well.

(3) Suppose $\varphi \colon A \to A$ is a separable isogeny. Here, we can compute $\deg \varphi = \#\ker \varphi(\overline{k})$, so

$$|\deg \varphi|_\ell = \left|\#(\ker \varphi)(\overline{k})\right|_\ell = \frac{1}{\#(\ker \varphi)(\overline{k})(\ell)},$$

where $(\ker \varphi)(\overline{k})(\ell)$ denotes the Sylow ℓ-subgroup of $(\ker \varphi)(\overline{k})$. However, $(\ker \varphi)(\overline{k})(\ell)$ is exactly the ℓ-power torsion killed by φ, so it is equal in size to $\operatorname{coker} T_\ell\varphi$ by examining the cokernel of this limit. However, by row-reducing the isomorphism $T_\ell\varphi \colon T_\ell A \to T_\ell A$, we see $[T_\ell A : \operatorname{im} T_\ell\varphi]$ is exactly equal to $\det T_\ell\varphi$

(4) Because any map $A \to A$ of k-varieties can be split into separable and inseparable pieces, and (2.2) is multiplicative in φ on both sides, we conclude that (2.2) holds for any isogeny.

[1] This fact is used to show that isogenies form a reflexive relation, so it can be considered as "basic" as that, though the correct proof requires an understanding of finite group schemes.

We are now ready to conclude, using Lemma 2.12. Let Q_φ be the characteristic polynomial of $V_\ell\varphi\colon V_\ell A \to V_\ell A$, and factor $P_\varphi(t) = \prod_{i=1}^{2\dim A}(t-\alpha_i)$ and $Q_\varphi(t) = \prod_{i=1}^{2\dim A}(t-\beta_i)$. Indeed, we know that these are both monic polynomials of degree $2\dim A$, by their constructions.

For our application, observe that $f \mapsto \deg f$ is a polynomial map by Proposition 2.11, and $f \mapsto \det V_\ell\varphi$ is a polynomial map because $\mathrm{End}(V_\ell A) \to \mathbb{Q}$ is a polynomial map, and both are multiplicative functions. Thus, for any $F \in \mathbb{Z}[t]$ with leading coefficient $c \neq 0$, Lemma 2.13 and (2.2) achieve

$$\left|\prod_{i=1}^{2\dim A} F(\alpha_i)\right|_\ell = |d(c)|_\ell \,|\deg F(\varphi)|_\ell = |d(c)|_\ell \,|\det V_\ell\varphi|_\ell = \left|\prod_{i=1}^{2\dim A} F(\beta_i)\right|_\ell,$$

so Lemma 2.12 implies $P_\varphi = Q_\varphi$, as desired. ∎

We now use our newfound power to prove some results which are quite non-obvious using the original definition P_φ.

Corollary 2.15. *Fix an endomorphism $\varphi\colon A \to A$ of an abelian k-variety A. Then P_φ has integer coefficients.*

Proof. We follow [EGM, Corollary 12.10]. Note that the ring $\mathrm{End}^0(A)$ is finite and hence integral over $\mathbb{Z}$, so $\varphi \in \mathrm{End}^0(A)$ is integral, so we can find a monic polynomial $P \in \mathbb{Z}[x]$ such that $P(\varphi) = 0$. Choosing any prime ℓ not divisible by $\operatorname{char} k$, functoriality of V_ℓ then implies $P(V_\ell\varphi) = 0$, but this implies that all eigenvalues of $V_\ell\varphi$ are algebraic integers. Thus, the coefficients of P_φ are algebraic integers by Proposition 2.14, so they are integers because $P_\varphi \in \mathbb{Q}[x]$. ∎

Corollary 2.16. *Fix an endomorphism $\varphi\colon A \to A$ of an abelian k-variety A, and factor $P_\varphi(t) = \prod_{i=1}^{2\dim A}(t-\alpha_i)$. Then*

$$P_{\varphi^m}(t) = \prod_{i=1}^{2\dim A} (t - \alpha_i^m).$$

Proof. Choose any prime ℓ not divisible by $\operatorname{char} k$, and set $d \coloneqq \dim A$ for brevity. In light of Proposition 2.14, P_φ and P_{φ^m} are the characteristic polynomials of the linear transformations $V_\ell\varphi$ and $V_\ell\varphi^m = (V_\ell\varphi)^m$, respectively. Thus, we are trying to show that the multiset of eigenvalues of $(V_\ell\varphi)^m$ is given by $\{\alpha_1^m, \dots, \alpha_{2d}^m\}$, which is just a linear algebra: passing to the algebraic closure, we may write $V_\ell\varphi$ as a triangular matrix $2d \times 2d$ matrix M, where the eigenvalues are on the diagonal. But then $(V_\ell\varphi)^m$ is given by the matrix M^m, and the eigenvalues are still on the diagonal and the mth power of the eigenvalues on the diagonal of M. ∎

Example 2.17. *We continue in the context of Example 2.8. Here is an alternate computation of P_φ: factor $P_\varphi(x) = (x-\alpha)(x-\beta)$. Then we see*

$$(x-1)^2 = P_{\mathrm{id}_E}(x) = P_{\varphi^3}(x) = \left(x-\alpha^3\right)\left(x-\beta^3\right),$$

so $\alpha^3 = \beta^3 = 1$. However, $\alpha = 1$ or $\beta = 1$ implies $\deg(\varphi - [1]) = 0$, which is false because $\varphi - [1]$ has finite kernel (which we computed). Thus, we must have $\{\alpha, \beta\} = \left\{\zeta_3, \zeta_3^2\right\}$, so $P_\varphi(x) = x^2 + x + 1$ again.

3. Rationality

With a firm understanding of the characteristic polynomial, we are now ready to approach our proof of Theorem 1.4. We follow [EGM, Chapter 16].

3.1. **The Frobenius.** Throughout, $k \coloneqq \mathbb{F}_q$ is a finite field, where q is a prime-power p^ν. We let A denote an abelian k-variety. We would like to count $A\left(\mathbb{F}_{q^m}\right)$ as m varies. Intuitively speaking, we see that an $\overline{\mathbb{F}_q}$-point $(a_1, \dots, a_n) \in A$ comes from $\mathbb{F}_q$ if and only if each coordinate a_i lives in $\mathbb{F}_q$, which is equivalent to $a_i^q = a_i$. Thus, we want a notion of Frobenius for our varieties.

Definition 3.1 (Frobenius)**.** *Let X be a variety over the finite field $k \coloneqq \mathbb{F}_q$. Then the Frobenius morphism $\pi_X\colon X \to X$ is defined as follows.*

- *π_X is the identity on the topological space.*
- *$\pi_X^\sharp\colon \mathcal{O}_X \to \mathcal{O}_X$ is the qth-power map.*

Note that $\pi_X\colon X \to X$ is a morphism of k-schemes because the qth-power map fixes k.

Remark 3.2. *It is more typical to define the (relative) Frobenius as the pth-power map and define the above Frobenius as some kind of power of the above map, but we will have no need for this construction.*

Remark 3.3. *We note that the degree of the Frobenius map $\pi_X\colon X \to X$ is $q^{\dim X}$. Indeed, we want to compute the degree of the $\mathbb{F}_q$-algebra field extension $K(X) \to K(X)$ given by taking qth powers. But $K(E)$ has transcendence degree $\dim X$ over $\mathbb{F}_q$, this transcendence degree will give degree $q^{\dim X}$.*

Remark 3.4. *When A is an abelian variety over $k \coloneqq \mathbb{F}_q$, we see that $\pi_A\colon A \to A$ is a map of k-schemes fixing the rational point $0_A \in A(k)$. It follows that π_A is an endomorphism.*

Let's now make the above motivation rigorous.

Lemma 3.5. *Let X be a variety over a finite field $k \coloneqq \mathbb{F}_q$. Then $X(k)$ is the set of points fixed in $X(\overline{k})$ by π_X.*

Proof. We are showing that a geometric point $\overline{x} \in X(\overline{k})$ is a rational point if and only if $\pi_X(\overline{x}) = \overline{x}$. Translating to scheme theory, if the maps $\operatorname{Spec}\overline{k} = \operatorname{Spec}\overline{k} \xrightarrow{\overline{x}} X$ and $\operatorname{Spec}\overline{k} \xrightarrow{\pi_k} \operatorname{Spec}\overline{k} \xrightarrow{\overline{x}} X$ agree, then $\overline{x}$ factors uniquely through $\operatorname{Spec} k$; here $\pi_k\colon \overline{k} \to \overline{k}$ is the qth-power map.

Thus, we would like to show that the scheme $\operatorname{Spec} k$ is the coequalizer of the maps $\pi_k, \mathrm{id}\colon \operatorname{Spec}\overline{k} \to \operatorname{Spec}\overline{k}$. This can be checked on affine schemes, whereupon taking the opposite category we are trying to show that k is the equalizer of the maps $\pi_k, \mathrm{id}\colon \overline{k} \to \overline{k}$. Well, for any k-algebra A equipped with a map $f\colon A \to \overline{k}$ such that $f = \pi_k \circ f$, we see that $\pi_k(f(a)) = f(a)$, so $f(a) \in \overline{k}$ is fixed by the qth-power map, so $f(a) \in k$, so f does indeed factor uniquely through k. ∎

Proposition 3.6. *Let A be an abelian variety over a finite field $k \coloneqq \mathbb{F}_q$. Then*

$$P_{\pi_A^m}(1) = \#A\left(\mathbb{F}_{q^m}\right)$$

for any positive integer m. Note that π_A^m is an endomorphism by Remark 3.4.

Proof. Replacing A by $A_{\mathbb{F}_{q^m}}$, we may assume that $k = \mathbb{F}_{q^m}$; notably, we can check by hand that the Frobenius of $A_{\mathbb{F}_{q^m}}$ is π_A^m because these are both the q^m-power map on sheaves. Namely, we now want to show that $P_\pi(1) = \#A(k)$.

To begin, the definition of P_π yields $P_\pi(1) = \deg(\pi - \mathrm{id})$. On the other hand, Lemma 3.5 implies that $A(k)$ consists of the geometric points $x \in A(\overline{k})$ such that $\pi_A(x) = x$, which is equivalent to $x \in \ker(\pi_A - \mathrm{id})(\overline{k})$. Thus, we are trying to show

$$\deg(\pi_A - \mathrm{id}) \stackrel{?}{=} \#\ker(\pi_A - \mathrm{id})(\overline{k}),$$

so we are trying to show that $\pi_A - \mathrm{id}$ is separable. In fact, we claim that $\pi_A - \mathrm{id}$ is étale. We do know that $\pi_A - \mathrm{id}$ is an isogeny because it has finite kernel: indeed, it has kernel $A(k)$, which is finite because A is a finite-type scheme over a finite field.

But now, to show étale, we observe for psychological reasons that it is enough to show that $\pi_A - \mathrm{id}$ is étale at 0, which is fixed. Now, we can merely show that $\pi_A - \mathrm{id}$ is an isomorphism on Zariski cotangent spaces $\mathfrak{m}_0/\mathfrak{m}_0^2 \to \mathfrak{m}_0/\mathfrak{m}_0^2$, where $y = (\pi_A - \mathrm{id})(x)$; this is enough by [Har77, Proposition III.10.4], upon passing to the algebraic closure. But π_A is the qth-power map and will thus annihilate everything in the cotangent space, so we are only looking at $-\mathrm{id}$, which is of course an isomorphism. ∎

Corollary 3.7. *Let A be an abelian variety over a finite field $\mathbb{F}_q$. Factor $P_{\pi_A}(t) = \prod_{i=1}^{2\dim A}(t - \alpha_i)$. Then*

$$\#A\left(\mathbb{F}_{q^m}\right) = \prod_{i=1}^{2\dim A}\left(1 - \alpha_i^m\right)$$

for any positive integer m.

Proof. In light of Proposition 3.6, it is enough to note that

$$P_{\pi_A^m}(t) = \prod_{i=1}^{2\dim A}\left(t - \alpha_i^m\right)$$

by Corollary 2.16 and plug in 1. ∎

Example 3.8. *Work in the context of Example 2.1, and set* $k \coloneqq \mathbb{F}_5$. *Note* $P_{\pi_E}(0) = 5$ *by Remark 3.3. Further, we see*

$$E(\mathbb{F}_5) = \{[0:1:0], [0:1:1], [0:4:1], [2:2:1], [2:3:1], [4:0:1]\}$$

has cardinality 6, *so* $P_{\pi_E}(1) = 6$ *by Corollary 3.7. Interpolating, we see* $P_{\pi_E}(x) = x^2 + 5$, *so Corollary 3.7 promises*

$$\#E\left(\mathbb{F}_{q^m}\right) = \left(1 - (-i\sqrt{5})^m\right)\left(1 - (i\sqrt{5})^m\right) = \begin{cases} \left(5^{m/2} + 1\right)^2 & \text{if } m \equiv 0 \pmod 2, \\ 5^m + 1 & \text{if } m \equiv 1 \pmod 2. \end{cases}$$

For example, one can compute $\#E\left(\mathbb{F}_{5^{10}}\right) = 9771876 = 3126^2$ *and* $\#E\left(\mathbb{F}_{5^{11}}\right) = 48828126 = 5^{11} + 1$.

3.2. **Rationality.** In this section, we use linear algebra to prove rationality (as in Theorem 1.3) for abelian varieties. To motivate ourselves, we recast Corollary 3.7 into linear algebra.

Lemma 3.9. *Let* A *be an abelian variety over a finite field* $\mathbb{F}_q$ *of dimension* d. *Then*

$$\#A\left(\mathbb{F}_{q^m}\right) = \sum_{j=0}^{2d} (-1)^j \operatorname{tr}\left(\pi_A \mid \wedge^j V_\ell A\right),$$

where $\alpha_I \coloneqq \prod_{i \in I} \alpha_i$.

Proof. Expanding Corollary 3.7 fully, one sees

$$\#A\left(\mathbb{F}_{q^m}\right) = \prod_{i=1}^{2d} (1 - \alpha_i^m) = \sum_{I \subseteq \{1,\ldots,2d\}} (-1)^{\#I} \alpha_I^m.$$

However, a computation with exterior powers is able to show that

$$\operatorname{tr}\left(\pi_A \mid \wedge^j V_\ell A\right) = \sum_{\substack{I \subseteq \{1,\ldots,2d\} \\ \#I = j}} \alpha_I$$

We will not show this rigorously, but here is a sketch: it is easy to see if π_A is diagonalizable because π_A remains diagonalizable on $\wedge^j V_\ell A$ with eigenvectors given by wedge products of eigenvectors. From here, one could argue that diagonal operators are Zariski dense to finish or generalize the given argument to work with upper-triangular matrices instead of diagonal ones. Anyway, the point is that

$$\#A\left(\mathbb{F}_{q^m}\right) = \sum_{j=0}^{2d} \left((-1)^j \prod_{\substack{I \subseteq \{1,\ldots,2d\} \\ \#I = j}} \alpha_I \right) = \sum_{j=0}^{2d} (-1)^j \operatorname{tr}\left(\pi_A \mid \wedge^j V_\ell A\right),$$

as desired. ∎

It is remarkable that Lemma 3.9 has essentially erased the characteristic polynomial from view, though of course it is present in the background. Anyway, to continue, we require the following linear algebra result.

Lemma 3.10. *Fix an endomorphism* $\varphi \colon V \to V$ *of a finite-dimensional* k*-vector space* V. *Then*

$$\exp\left(\sum_{m=1}^{\infty} \operatorname{tr}\left(\varphi^m \mid V\right) \frac{t^m}{m} \right) = \det\left(\mathrm{id} - \varphi t \mid V\right)^{-1}$$

as formal power series in t.

Proof. We follow [Har77, Lemma C.4.1]. The proof is by induction on $\dim V$. If $\dim V = 1$, then φ is a scalar, say λ, so the equality reads

$$\exp\left(\sum_{m=1}^{\infty} \frac{(\lambda t)^m}{m} \right) = \exp(-\log(1 - \lambda t)) = \frac{1}{1 - \lambda t},$$

as needed. For the induction, let the left-hand side of the desired equation be $L(\varphi, V)$, and let the right-hand side by $R(\varphi, V)$. For an exact sequence

$$0 \to V' \to V \to V'' \to 0$$

of vector spaces, suppose $\varphi\colon V \to V$ is an operator fixing V'; in general, we can let V' be the subspace spanned by a single eigenvector of φ. Now, φ is also an operator on V'', and we see that $L(\varphi, V) = L(\varphi, V')L(\varphi, V'')$ because trace is additive, and $R(\varphi, V) = R(\varphi, V')R(\varphi, V'')$ because determinant is multiplicative. (Explicitly, one can observe that the short exact sequence splits and note that replacing φ with the operator given by the splitting has the same traces and determinants.) Thus, the inductive hypothesis gives $R(\varphi, V') = L(\varphi, V')$ and $R(\varphi, V'') = L(\varphi, V'')$, so we conclude. ∎

We are finally ready to prove Theorem 1.4.

Theorem 1.4 (Rationality)**.** *Let A be an abelian variety over a finite field $\mathbb{F}_q$ of dimension d. Then one has*

$$Z(A,t) = \frac{P_1(t)P_3(t)\cdots P_{2d-1}(t)}{P_0(t)P_2(t)\cdots P_{2d}(t)}$$

where each $P_j(t)$ is a polynomial with integer coefficients, depending on the eigenvalues of the Frobenius $\pi_A\colon A \to A$.

Proof. Using (1.1), we may plug in Lemma 3.9 to see

$$\begin{aligned} Z(A,t) &= \exp\left(\sum_{m=1}^{\infty} \#A\left(\mathbb{F}_{q^m}\right)\frac{t^m}{m}\right) \\ &= \exp\left(\sum_{m=1}^{\infty}\sum_{j=0}^{2d}(-1)^j \operatorname{tr}\left(\pi_A \mid \wedge^j V_\ell A\right)\frac{t^m}{m}\right) \\ &= \prod_{j=0}^{2d}\exp\left(\sum_{m=1}^{\infty}\operatorname{tr}\left(\pi_A \mid \wedge^j V_\ell A\right)\frac{t^m}{m}\right)^{(-1)^j} \\ &= \prod_{j=0}^{2d}\det(\mathrm{id} - t\pi_A \mid \wedge^j V_\ell A)^{(-1)^{j+1}}, \end{aligned}$$

where we have used Lemma 3.10 in the last equality. Thus, using the discussion of the eigenvalues of π_A from Lemma 3.9, we see that

$$P_j(t) \coloneqq \det(\mathrm{id} - t\pi_A \mid \wedge^j V_\ell A) = \prod_{\substack{I\subseteq\{1,\dots,2d\}\\ \#I=j}}(1 - t\alpha_I),$$

which finishes the rationality of $Z(A,t)$ upon plugging in for $P_j(t)$. Lastly, we see that the coefficients of $P_j(t)$ are rational because any Galois automorphism will merely permute $\{\alpha_i\}_{i=1}^n$ and thus also permute $\{\alpha_I\}_{\#I=j}$. Additionally, all the coefficients are algebraic integers, so P_j as integer coefficients. ∎

Remark 3.11. *To prove the rest of Theorem 1.3 for abelian varieties, one needs information about the eigenvalues α_i of π_A. For example, it might appear that one can use Theorem 1.4 to produce the functional equation purely formally, but one (approximately) needs to know that all the α_i have magnitude $\sqrt{q}$ for this argument to go through, which is essentially the Riemann hypothesis. Anyway, showing these facts is nonetheless easier in the case of abelian varieties than in general, due to the theory of the Rosati involution; see [Mil08, Section I.14], for example.*

4. Elliptic Curves

For a source of examples, we turn our attention to elliptic curves, where we will be able to complete the proof of the Weil conjectures. We follow [Sil09, Section V.2].

4.1. **The Weil Conjectures.** Let E be an elliptic curve over a finite field $\mathbb{F}_q$. In this dimension-1 case, the difficulty of understanding eigenvalues described in Remark 3.11 collapses because there are only two eigenvalues, so we are able to achieve the remaining Weil conjectures.

Lemma 4.1. *Let E be an elliptic curve over a finite field $\mathbb{F}_q$. Then*

$$P_{\pi_E}(t) = t^2 - at + q$$

where $a \coloneqq (q+1) - \#E(\mathbb{F}_q)$. In particular, the eigenvalues of π_E have magnitude $\sqrt{q}$.

Proof. Note P_{π_E} is monic by definition. Also, $P_{\pi_E}(0) = \deg \pi_E$ by definition of P_{π_E}, and $\deg \pi_E = q$ by Remark 3.3. Thus, the story so far is that

$$P_{\pi_E}(t) = t^2 - at + q$$

for some integer $a \in \mathbb{Z}$. However, Proposition 3.6 tells us that $\#E(\mathbb{F}_q) = 1 - a + q$, from which the first claim follows.

For the last sentence, note that the eigenvalues α_1 and α_2 of π_E are roots of P_{π_E}, so the discussion above implies $\alpha_1\alpha_2 = q$. Now, we see $P_{\pi_E}(r) = \deg(\pi_E - r[1]) \geq 0$ for any $r \in \mathbb{Q}$, so continuity implies that $P_{\pi_E}(r) \geq 0$ for any $r \in \mathbb{R}$ also. Thus, P_{π_E} either has $\alpha_1 = \alpha_2$ (and so $\alpha_1 = \alpha_2 = \pm\sqrt{q}$) or has two roots in $\mathbb{C}$ which are conjugate (and so $|\alpha_1| = |\alpha_2| = \sqrt{q}$), but we are okay in either case. ∎

Theorem 4.2 (Riemann hypothesis)**.** *Let E be an elliptic curve over a finite field $\mathbb{F}_q$. Then the factorization in Theorem 1.4 is*

$$Z(E,t) = \frac{1 - at + qt^2}{(1-t)(1-qt)}$$

where $a \coloneqq (q+1) - \#E(\mathbb{F}_q)$. Furthermore, the roots of $P_1(t) = 1 - at + t^2$ have magnitude $q^{-1/2}$.

Proof. Let α_1 and α_2 be the eigenvalues of π_E. Using the description of $Z(E,t)$ provided by the proof of Theorem 1.4, we see $P_0(t) = 1 - t$ and $P_1(t) = (1 - t\alpha_1)(1 - t\alpha_2) = t^2 P_{\pi_E}(1/t)$ and $P_2(t) = (1 - qt)$. Combining this information with Lemma 4.1, we see

$$Z(E,t) = \frac{1 - at + t^2}{(1-t)(1-qt)}$$

where $a = (q+1) - \#E(\mathbb{F}_q)$. Now, the roots of $P_1(t)$ are $1/\alpha_1$ and $1/\alpha_2$, so they have magnitude $q^{-1/2}$ by Lemma 4.1. ∎

Theorem 4.3 (Functional equation)**.** *Let E be an elliptic curve over a finite field $\mathbb{F}_q$. Then, as formal power series,*

$$Z\left(E, q^{-1}t^{-1}\right) = Z(E,t).$$

Proof. This is purely formal from Theorem 4.2. Explicitly,

$$Z\left(E, q^{-1}t^{-1}\right) = \frac{1 - a \cdot \frac{1}{qt} + q \cdot \frac{1}{q^2t^2}}{\left(1 - \frac{1}{qt}\right)\left(1 - q \cdot \frac{1}{qt}\right)} = \frac{qt^2 - at + 1}{(qt-1)(t-1)} = Z(E,t),$$

which is what we wanted. ∎

4.2. **Counting Points.** As an application of our hard work, we note that we can in fact use these results to count points.

Corollary 4.4 (Hasse)**.** *Let E be an elliptic curve over a finite field $\mathbb{F}_q$. For any $m \geq 0$, we have*

$$|\#E(\mathbb{F}_q) - (q+1)| \leq 2\sqrt{q}.$$

Proof. By Lemma 4.1, we see that $a \coloneqq (q+1) - \#E(\mathbb{F}_q)$ is the sum of two complex numbers of magnitude $\sqrt{q}$, so $|a| \leq 2\sqrt{q}$. ∎

Example 4.5. *We work in the context of Example 2.1, and set $k \coloneqq \mathbb{F}_7$. Here is a table of values $\#E\left(\mathbb{F}_{7^m}\right)$ and their distance from $7^m + 1$.*

m	$\#E\left(\mathbb{F}_{7^m}\right)$	$(7^m+1) - \#E\left(\mathbb{F}_{7^m}\right)$	$\lfloor\sqrt{7^m}\rfloor$
1	12	−4	5
2	48	2	14
3	324	20	37
5	16572	236	259
10	282453168	22082	33614

Corollary 4.6. *Let E be an elliptic curve over a finite field $\mathbb{F}_q$. For each positive integer m, define $a_m \coloneqq q^m + 1 - \#E\left(\mathbb{F}_{q^m}\right)$, and set $a_0 \coloneqq 2$. Then, for any $m \geq 0$, one has*

$$a_{m+2} = a_1 a_{m+1} - q a_m.$$

Proof. Let α_1 and α_2 be the eigenvalues of π_E. By Corollary 3.7, we see

$$\#E\left(\mathbb{F}_{q^m}\right) = \left(1-\alpha_1^m\right)\left(1-\alpha_2^m\right) = (\alpha_1\alpha_2)^m - \alpha_1^m - \alpha_2^m + 1$$

for any $m \geq 1$. By Lemma 4.1, we see $\alpha_1\alpha_2 = q$, so rearranging the above equation gives $a_m = \alpha_1^m + \alpha_2^m$ for any $m \geq 1$, but we note that $2 = a_0 = \alpha_1 + \alpha_2$ as well. From here, proving the recurrence relation is purely formal: for any $m \geq 0$, we compute

$$\begin{aligned} a_{m+2} - a_1 a_{m+1} + q a_m &= \left(\alpha_1^{m+2} + \alpha_2^{m+2}\right) - \left(\alpha_1 + \alpha_2\right)\left(\alpha_1^{m+1} + \alpha_2^{m+1}\right) + q\left(\alpha_1^m + \alpha_2^m\right) \\ &= \left(\alpha_1^{m+2} + \alpha_2^{m+2}\right) - \left(\alpha_1^{m+2} + \alpha_2^{m+2}\right) - \alpha_1\alpha_2\left(\alpha_1^m + \alpha_2^m\right) + q\left(\alpha_1^m + \alpha_2^m\right) \\ &= 0, \end{aligned}$$

where in the last equality we have used the fact that $\alpha_1\alpha_2 = q$. ∎

Example 4.7. *We execute Corollary 4.6 in the context of Example 2.1 where $k \coloneqq \mathbb{F}_7$. One can compute*

$$\begin{aligned} E(\mathbb{F}_7) = \{&[0:1:0],[0:1:1],[0:6:1],[1:3:1],[1:4:1],[2:3:1], \\ &[2:4:1],[3:0:1],[4:3:1],[4:4:1],[5:0:1],[6:0:1]\}, \end{aligned}$$

so $\#E(\mathbb{F}_7) = 12$, as in Example 4.5. So we have $a_0 = 2$ and $a_1 = -4$, from which we get the following table.

$m+2$	$a_1 a_{m+1}$	$-7a_m$	a_{m+2}	$\#E\left(\mathbb{F}_{q^{m+2}}\right) = \left(7^{m+2}+1\right) - a_{m+2}$
2	16	−14	2	48
3	−8	28	20	324
4	−80	−14	−94	2496
5	376	−140	236	16572
6	−944	658	−286	117936
7	1144	−1652	−508	824052

References

[Wei49] André Weil. "Numbers of solutions of equations in finite fields". In: *Bulletin of the American Mathematical Society* 55.5 (1949), pp. 497–508.

[Har77] Robin Hartshorne. *Algebraic Geometry*. Graduate Texts in Mathematics, No. 52. New York: Springer-Verlag, 1977.

[Ras07] Sam Raskin. *The Weil Conjectures for Curves*. 2007. URL: https://math.uchicago.edu/~may/VIGRE/VIGRE2007/REUPapers/FINALFULL/Raskin.pdf.

[Mil08] James S. Milne. *Abelian Varieties (v2.00)*. Available at www.jmilne.org/math/. 2008.

[Sil09] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*. 2nd ed. Graduate Texts in Mathematics. Springer New York, NY, 2009. DOI: https://doi.org/10.1007/978-0-387-09494-6.

[Elb22] Nir Elber. *Abelian Varieties*. 2022. URL: https://dfoiler.github.io/notes/256A/paper.pdf.

[EGM] Bas Edixhoven, Gerard van der Geer, and Ben Moonen. *Abelian Varieties*. URL: http://van-der-geer.nl/~gerard/AV.pdf.