The Weil Conjectures for Abelian Varieties

Caleb Ji

Summer 2021

We will sketch Weil's proof of his famous conjectures for abelian varieties. Then we will explain how this can be used to deduce these statements for curves using the theory of the Jacobian. We follow [1].

Contents

1 Preliminaries

1.1 Basics of abelian varieties

In our conventions, we set a variety to be a geometrically reduced separated scheme of finite type over a field k (not necessarily algebraically closed). A group variety is a group object in the category of varieties.

Definition 1.1. *An* ***abelian variety*** *is a complete connected group variety.*

Automatically, abelian vaieties are smooth, geometrically connected, and geometrically irreducible. The prototypical example of an abelian variety is an elliptic curve. In general though, the equations used to define abelian varieties are extremely complex and cannot be used. We begin by showing that abelian varieties are abelian as groups and projective.

Proposition 1.2. *Abelian varieties are abelian.*

Sketch. The key point is the following lemma: if V is complete and $V \times W$ is geometrically irreducible, then any map $\alpha : V \times W \to U$ with $\alpha(V \times \{w_0\}) = \alpha(\{v_0\} \times W) = u_0$, then $\alpha = u_0$. This is used to show that any map between abelian varieties is the composition of a homomorphism and a translation. Indeed, if $\alpha(0) = 0$, apply the lemma to $\alpha(a_1, a_2) = \alpha(a_1 + a_2) - \alpha(a_1) - \alpha(a_2)$. In particular, the inverse map must be a homomorphism, implying that abelian varieties are indeed abelian. □

Let us now state the 'theorem of the cube' and the 'theorem of the square.'

Theorem 1.3 (The cube). *Let $(U, u_0), (V, v_0), (W, w_0)$ be complete geometrically irreducible varieties. Then if some invertible sheaf $\mathcal{L}$ on $U \times V \times W$ is trivial on the three 'faces', it is itself trivial.*

This can be used to prove:

Theorem 1.4 (The square). *For all invertible sheaves $\mathcal{L}$ on A and points $a, b \in A(k)$, we have*

$$t_{a+b}^*\mathcal{L} \otimes \mathcal{L} \cong t_a^*\mathcal{L} \otimes t_b^*\mathcal{L}.$$

In particular, $a \mapsto t_a^*\mathcal{L} \otimes \mathcal{L}^{-1} : A(k) \to \mathrm{Pic}(A)$ is a homomorphism, and if $\sum a_i = 0$, then $\otimes_i t_{a_i}^*\mathcal{L} = \mathcal{L}^n$. In terms of divisors, this means that the map

$$a \mapsto [D_a - D] : A(k) \to \mathrm{Pic}(A)$$

is a homomorphism. These ideas are used in the following proposition.

Proposition 1.5. *Abelian varieties are projective.*

Sketch. Recall that to give a projective embedding of a variety, one may give an ample divisor, or a complete linear system that separates points and tangent vectors. We first construct a divisor $D = \sum Z_i$ that separates 0 and tangents at 0. This is essentially done by taking hyperplanes which cut 0 off from other points/vectors and using the descending chain condition.

We now claim that $3D$ is very ample. Indeed, by the theorem of the square, the complete linear system defined by $3D$ includes

$$\sum Z_{i,a_i} + Z_{i,b_i} + Z_{i,-a_i-b_i}.$$

We can use such constructions to separate points and tangent vectors. □

Note that these sorts of arguments assume that k is algebraically closed. However, these results hold in general; see [1] Proposition I.6.6.

Finally, we define the Néron-Severi group of a complete smooth variety: $\mathrm{NS}(V) := \mathrm{Pic}(V)/\mathrm{Pic}^0(V)$. It is always finitely generated. For abelian varieties, the map $\mathcal{L} \mapsto \lambda_{\mathcal{L}}$ gives an injection $\mathrm{NS}(A) \hookrightarrow \mathrm{Hom}(A, A^\vee)$, which one can prove (following Tate) is a free $\mathbb{Z}$-module of rank $\leq 4\dim(A)^2$.

1.2 Isogenies and the Tate module

Definition 1.6. *An **isogeny** $f : A \to B$ of abelian varieties is a homomorphism of abelian varieties that is surjective and has finite kernel.*

Definition 1.7. *The **degree** of an isogeny $\alpha : A \to B$ is given by the degree $[k(A) : \alpha^*k(B)]$.*

Let α be an isogeny of degree d. Isogenies are flat. If α is separable, then it is étale outside of the ramification points. But the homogeneity of an abelian variety implies that if one point is ramified then they all are. So separable isogenies are étale. Furthermore, if k is algebraically closed, each fiber has cardinality d.

Theorem 1.8. *The map n_A, multiplicion by n on an abelian variety A of dimension g, is an isogeny of degree n^{2g}. Furthermore, n_A is étale if and only if $\mathrm{ch}(k) \nmid n$.*

For a proof, see [1], Theorem I.7.2. The idea is the following: we can find a symmetric very ample invertible sheaf $\mathcal{L}$ on A. Using the theorem of the cube we get that $(n_A)^*\mathcal{L} \cong \mathcal{L}^{n^2}$. Then translate this into the language of divisors.

This allows us to define the l-adic Tate module as follows. Let $A_n(k)$ be the kernel of n_A.

Definition 1.9. *Fix l to be a prime not equal to $\mathrm{ch}(k)$. Then we define the l-adic Tate module as*

$$T_l(A) = \varprojlim A_{l^n}(k^{sep}).$$

Furthermore, define $V_l(A) = T_l(A) \otimes_{\mathbb{Z}} \mathbb{Q}$.

1.3 Sketch of the elliptic curve case

We will briefly sketch the proof of the Weil conjectures for elliptic curves. Full details may be found in .

Let X be a smooth projective variety of dimension n over $\mathbb{F}_q$. We define its zeta function by

$$Z(X,t) := \exp\left(\sum_{r=1}^{\infty} N_r \frac{t^r}{r}\right),$$

where N_r is the number of closed points of X where considered over $\mathbb{F}_{q^r}$. If $E/\mathbb{F}_q$ is an elliptic curve, then we wish to show that

$$Z(E,t) = \frac{(1-\alpha t)(1-\beta t)}{(1-t)(1-qt)},$$

where $|\alpha| = |\beta| = \sqrt{q}$.

Let π be the Frobenius endomorphism. Then one shows that $1-\pi$ is separable, and thus

$$|E(\mathbb{F}_q)| = |\ker(1-\pi)| = \deg(1-\pi).$$

Furthermore, π induces an endomorphism π_l of the Tate module $T_l(E)$. The characteristic polynomial of π_l is given by $T^2 - \mathrm{Tr}(\phi_l)T + \det(\phi_l)$. One shows that $\det(\pi_l) = \deg(\phi) = q$, while $\mathrm{Tr}(\pi_l) = 1 + \deg(\pi) - \deg(1-\pi) = 1 + q - |E(\mathbb{F}_q)|$, the famous “trace of Frobenius." Factoring the characteristic polynomial as $(T-\alpha)(T-\beta)$, we get $|\alpha| = \beta| = \sqrt{q}$. We do the same for π^n and points over $\mathbb{F}_{q^n}$ and factor it as $(T-\alpha^n)(T-\beta^n)$.

The upshot is that $|E(\mathbb{F}_{q^n})| = \deg(1-\pi^n) = \det(1-\pi_l^n) = (1-\alpha^n)(1-\beta^n)$. From here it is easy to compute the zeta function by taking its $\log$.

2 The Weil conjectures for abelian varieties

2.1 The characteristic polynomial of an endomorphism

Let $A/\mathbb{F}_q$ be an abelian variety. The existence of the Tate module $T_l(A)$ allows us to carry out a similar plan as the one outlined above for elliptic curves. The first order of business is to carefully define the characteristic polynomial of an endomorphism of A. Recall that for elliptic curves, it is literally the characteristic polynomial of the corresponding action on the Tate module. However, to show this is well-defined, we will instead define it in the following way.

Theorem 2.1. *Take $\alpha \in \operatorname{End}(A)$ where A is an abelian variety of dimension g. Then there is a unique monic polynomial $P_\alpha(x) \in \mathbb{Z}[x]$ such that $P_\alpha(r) = \deg(\pi - r)$. Then P_α is the **characteristic polynomial** of α.*

For a proof, see Theorem I.10.9 in [1]. One first shows that $\alpha \mapsto \deg(\alpha)$ is a polynomial function of degree $2g$. We now have the following proposition.

Proposition 2.2. *For all primes $l \neq \operatorname{ch}(k)$, we have that P_α is the characteristic polynomial of α acting on the Tate module $V_l A$.*

Here, we set $\deg(\alpha) = 0$ if α is not an isogeny. For a proof of this proposition, see [1], Proposition I.10.20.

2.2 The easy half

As usual, let π be the Frobenius. We factor

$$P_\pi(X) = \prod_{i=1}^{2g} (X - \alpha_i).$$

Then the Weil conjectures, modulo the functional equation, essentially boil down to the following statements.

Theorem 2.3. *(a) $N_m = \prod_{i=1}^{2g}(1 - \alpha_i^m)$.*
(b) $|a_i| = \sqrt{q}$. (Riemann hypothesis)

We will now prove (a) and, assuming (b), deduce the rationality of the zeta function. Part (b) is more difficult, but we note that in the case of elliptic curves it was trivial. Indeed, in this case there are only two roots which must be complex conjugates (since the trace is real) that multiply to q; hence they have absolute value $\sqrt{q}$.

Proof of (a). It suffices to do the case $m = 1$; that is, show that $N_1 = P_\pi(1)$. Since $P_\pi(1) = \deg(\pi - 1)$ and $N_1 = |\ker(1 - \pi)|$, it suffices to show that $\pi - 1$ is étale. It suffices to check this at 0, which can be done by calculating the differential. □

Note that we can now prove the following Hasse-Weil type bound:

$$|N_m - q^{mg}| \leq 2g \cdot q^{m(g-1/2)} + (2^{2g} - 2g - 1)q^{m(g-1)}.$$

This is actually very simple: simply expand the product formula given by (a) and note that the dominating term is q^{mg}. The rest follows from an easy triangle inequality bound.

Finally, we can express the zeta function as

$$Z(A,t) := \exp\left(\sum_{r\geq 1} N_r \frac{t^r}{r}\right) = \frac{P_1(t)\cdots P_{2g-1}(t)}{P_0(t)P_2(t)\cdots P_{2g}(t)},$$

where $P_r(t) = \prod_{i_1<\cdots<i_r}(1-a_{i_j}t)$. This follows from a direct calculation. We will not verify the functional equation here and instead focus on the Riemann hypothesis. For this, we need to introduce more general machinery regarding abelian varieties.

2.3 The dual abelian variety, polarizations, and the Rosati involution

The dual abelian variety, also known as the Picard variety, is an abelian variety $A^\vee$ that parametrizes the elements of $\mathrm{Pic}^0(A)$. Let us give a proper definition.

Definition 2.4. *Let $(A^\vee, \mathcal{P})$ be a pair where $\mathcal{P}$ is an invertible sheaf on $A \times A^\vee$. Assume that $\mathcal{P}|_{A\times\{b\}} \in \mathrm{Pic}^0(A_b)$ and $\mathcal{P}|_{\{0\}\times A^\vee}$ is trivial. Then $A^\vee$ is the **dual abelian variety** of A and $\mathcal{P}$ is the Poincaré sheaf if $(A^\vee, \mathcal{P})$ satisfies the following universal property. For every other such pair $(T, \mathcal{L})$, there is a unique regular map $\alpha : T \to A$ such that $(1\times\alpha)^*\mathcal{P} \cong \mathcal{L}$.*

In more conceptual terms, $(A^\vee, \mathcal{P})$ represents the functor sending a variety T to the set of line bundles on A parameterized by T.

The construction of the dual abelian variety is a special case of the construction of the Picard scheme, which was famously done by Grothendieck. However, even this special case is rather involved; one may consult [1] I.8.

Definition 2.5. *A **polarization** λ of an abelian variety is an isogeny $A \to A^\vee$ such that, over $\overline{k}$, we have that λ becomes of the form $\lambda_{\mathcal{L}}$ for some ample sheaf $\mathcal{L}$ on $A_{\overline{k}}$. If the degree of a polarization is 1, then λ is called a **principal polarization**.*

Recall that $\lambda_{\mathcal{L}} : A(k) \to \mathrm{Pic}(A)$ is defined by $\lambda_{\mathcal{L}}(a) = t_a^*\mathcal{L}\otimes\mathcal{L}^{-1}$. In fact, $\mathrm{Pic}^0(A)$ may be defined as those $\mathcal{L}$ for which $\lambda_{\mathcal{L}} = 0$.

Let us see what all this means for elliptic curves. Recall that elliptic curves come with a basepoint (at infinity; let us thus denote one by (E, P_0). The dual abelian variety in this case coincides with E, and the map $P \mapsto P - P_0$ gives at least a group isomorphism between E and $\mathrm{Pic}^0(E)$. This suggests why polzarized abelian varieties (as opposed to just abelian varieties) may be a good generalization of elliptic curves.

Given an isogeny $\alpha : A \to B$, there is a map $\beta : B \to A$ such that $\beta\circ\alpha = n$. Thus, a polrization has an inverse in $\mathrm{Hom}(A^\vee, A)\otimes\mathbb{Q}$.

Definition 2.6. *Let $\lambda : A \to A^\vee$ be a polarization on A. Then the **Rosati involution** on $\mathrm{End}(A)\otimes\mathbb{Q}$ corresponding to λ is*

$$\alpha \mapsto \alpha^\dagger = \lambda^{-1}\circ\alpha^\vee\circ\lambda.$$

The following theorem is key.

Theorem 2.7. *The bilinear form*

$$\langle\alpha,\beta\rangle \mapsto \mathrm{Tr}(\alpha\circ\beta^\dagger)$$

is positive definite.

2.4 The Riemann hypothesis for abelian varieties

We wish to show that $|a_i| = \sqrt{q}$. This follows from the next two lemmas.

Lemma 2.8. *Fix a Rosati involution $\dagger$ on $\mathrm{End}(A) \otimes \mathbb{Q}$. Then we have $\pi^\dagger \circ \pi = q_A$.*

Lemma 2.9. *If $\alpha^\dagger \circ \alpha = r$ for some integer r, then for any root $a \in \mathbb{C}$ of P_α, we have $|a|^2 = r$.*

Proof of Lemma 2.8. See Lemma II.1.2 in [1]. Here is a sketch. Let D be the ample divisor defining the polarization λ, so $\lambda(a) = [D_a - D]$. Then we wish to show that

$$\pi^\vee \circ \lambda \circ \pi = q\lambda.$$

We have $LHS = \pi^*[D_\pi(a) - D]$. Note that if $D = \mathrm{div}(f)$, then π^* sends this to $\mathrm{div}(f \circ \pi) = \mathrm{div}(f^q) = q\,\mathrm{div}(f)$. This explains where the factor of q comes from. □

Proof of Lemma 2.9. See Lemma II.1.3 in [1]. The main input is Theorem 2.7. □

3 Jacobians and the Weil conjectures for curves

3.1 Construction of the Jacobian

The classical theory of Jacobians over $\mathbb{C}$ is beautiful, but we are working over finite fields here. We will begin by constructing the Jacobian of a curve, an abelian variety that reflects some of the curve's important properties. In particular, the Frobenius on the curve induces the Frobenius on its Jacobian. We can then use the Riemann hypothesis for the Jacobian to prove the Riemann hypothesis for the curve we started with. It is worth pointing out that the Jacobian of an elliptic curve coincides with the elliptic curve itself, so the arguments are simplified in this case.

Let C be a smooth projective curve over k. For simplicity, we assume that $C(k)$ is nonempty; see [1], III.1 for what happens otherwise. We wish to construct the Jacobian J such that $J(k) = \mathrm{Pic}^0(C)$. In fact, consider the following functor $P_C^0(-)$:

$$P_C^0(T) = \mathrm{Pic}^0(C \times T)/q^* \,\mathrm{Pic}^0(T).$$

Then the Jacobian J represents the functor P_C^0. We sketch the construction when $k = \overline{k}$. Define $C^{(r)}$ to be C^r/S_r; note that this can be written as $\mathrm{Div}^r(C)$: the effective divisors of degree r. The Jacobian J will be birational to $C^{(r)}$.

Fix $P \in C(k)$ and take $D, D' \in C^{(g)}$. By the Riemann-Roch theorem, we have that $h^0(D + D' - gP) \geq 1$, and in fact equality holds for an open subset of $C^{(g)} \times C^{(g)}$. Then we can define a rational multiplication map $C^{(g)} \times C^{(g)} \to C^{(g)}$ which is well-defined on this open subset. Then arguments of Weil allow us to upgrade this $C^{(g)} \dashrightarrow J$ to an abelian variety with an agreeing addition law.

We now collect some results regarding the relation between C and its Jacobian J without proof (see [1], III.2). First, we have a canonical isomorphism between the tangent space at 0 to the Jacobian and the differentials: $T_0(J) \cong H^1(C, \mathcal{O}_C)$. Second, fix $P \in C(k)$ and consider the symmetric invertible sheaf $\mathcal{L}^P = \mathcal{L}(\Delta - C \times \{P\} - \{P\} \times C)$ on $C \times C$. This defines a map $f^P : C \to J$ which sends $Q \mapsto \mathcal{L}(Q) \otimes \mathcal{L}(P)^{-1}$. Note that in terms of divisors, this really just sends Q to $[Q - P]$. Then f^P is a closed immersion and induces an isomorphism $\Gamma(J, \Omega_J^1) \cong \Gamma(C, \Omega_C^1)$.

3.2 The intersection number formula and the Riemann hypothesis

Let C be a smooth complete curve with Jacobian J. A map $\alpha : C \to C$ induces an endomorphism $\alpha' \in \operatorname{End}(J)$ such that $f^P \circ \alpha = \alpha' \circ f^P$ for all $P \in C(\overline{K})$. The key is the following intersection number formula.

Proposition 3.1. *For $\alpha \in \operatorname{End}(C)$, we have*

$$(\Gamma_\alpha \cdot \Delta) = 1 - \operatorname{Tr}(\alpha') + \deg(\alpha).$$

To show this, we write $f = f^P$ and have the following commutative diagram.

$$\begin{tikzcd}
C \arrow[r, "f\times f"] \arrow[d, "\Delta"'] & C \times C \arrow[d, "\Delta\times\Delta"] & \\
J \arrow[r, "f"'] & J \times J \arrow[r, "1\times\alpha'"'] & J \times J
\end{tikzcd}$$

We consider the sheaf $\mathcal{L}'(\Theta) := \mathcal{L}(m^*\Theta - \Theta \times J - J \times \Theta)$ on $J \times J$. We compute the degree of this sheaf by going around the commutative diagram in two ways. It takes nontrivial results to make the calculation; see [1], III.11.

We now complete the proof. Let α be the Frobenius on C; then α' is the Frobenius on J. Then the LHS of Proposition 3.1 is N and the degree of α is q. Finally, by the result for abelian varieties, the characteristic polynomial of the Frobenius of J acting on $T_l J$ is a polynomial of degree $2g$ whose roots have absolute value $\sqrt{q}$. Thus, we have the Hasse-Weil bound

$$|N - q - 1| \leq 2g\sqrt{q}.$$

The Riemann hypothesis for curves follows easily from this (see for example my exposition of the Weil conjectures for curves).

3.3 Connection with étale cohomology

It makes sense to explain what we have done in terms of étale cohomology. Recall that $f^* : \Gamma(J, \Omega^1_J) \cong \Gamma(C, \Omega^1_C)$ is an isomorphism; one can use this or other methods to show that we also get an isomorphism $H^1(J, \mathcal{O}_J) \cong H^1(C, \mathcal{O}_C)$. Recalling that the first étale cohomology group is given by homomorphisms from the étale fundamental group, we also get an induced isomorphism $H^1_{et}(J, \mathbb{Z}_l) \cong H^1_t(C, \mathbb{Z}_l)$. Furthermore, we can write $H^1_{et}(J, \mathbb{Z}_l) \cong (T_l J)^\vee$.

Now we can rewrite Proposition 3.1 as

$$\Gamma_\alpha \cdot \Delta = \sum_{i=0}^{2} (-1)^i \operatorname{Tr}(\alpha | H^i_{et}(C, \mathbb{Z}_l)).$$

This statement generalizes to Grothendieck's trace formula, which applies to all varieties over finite fields (and constructible sheaves, etc.) As we have seen, in the case of curves it gives the Hasse-Weil bound and thus the Riemann hypothesis assuming the result for abelian varieties. It is not so simple for general varieties. However, it does lead to a proof of the other Weil conjectures relatively straightforwardly.

References

[1] James Milne. *Abelian Varieties*, v 2.0, 2008. Available at www.jmilne.org/math/.

[2] Robin Hartshorne. *Algebraic Geometry*. Springer Science+Business Media, Inc., 1977.

[3] Sam Raskin. *The Weil Conjectures for Curves*. Expository notes, retrieved online. https://math.uchicago.edu/~may/VIGRE/VIGRE2007/REUPapers/FINALFULL/Raskin.pdf