Intersection Theory on Surfaces and Riemann Hypothesis for Curves

David Bai

November 2022

1 The Weil Conjectures

As is mandatory for an article with this title, let's state the Weil conjectures: Let X be an n-dimensional projective variety over $\mathbb{F}_q$. Its Hasse-Weil ζ-function is the formal expression

$$\zeta(X,s) = \exp\left(\sum_{m=1}^{\infty} \frac{1}{m} \# X(\mathbb{F}_{q^m}) q^{-ms}\right).$$

Theorem 1.1 (Weil Conjectures). *Suppose X is nonsingular. Then:*

(i) (Rationality) There exists polynomials $P_0(T),\dots,P_{2n}(T) \in \mathbb{Z}[T]$ with constant coefficients 1 such that

$$\zeta(X,s) = \frac{P_1(q^{-s})\cdots P_{2n-1}(q^{-s})}{P_0(q^{-s})\cdots P_{2n}(q^{-s})}.$$

Furthermore, $P_0(T) = 1 - T, P_{2n}(T) = 1 - q^n T$.

(ii) (Functional equation) There is some integer $E = E(X)$ (the "Euler characteristic" of X) such that $\zeta(X, n-s) = \pm q^{nE/2-Es}\zeta(X,s)$. Consequently, if we let $P_i(T) = \prod_j (1 - \alpha_{i,j}T), 1 \le i \le 2n-1$ for some $\alpha_{i,j} \in \mathbb{C}$, then the tuple $(\alpha_{2n-i,1}, \alpha_{2n-i,2}, \dots)$ can be obtained by reordering $(q^n/\alpha_{i,1}, q^n/\alpha_{i,2}, \dots)$ for all i.

(iii) (Riemann hypothesis) $|\alpha_{i,j}| = q^{i/2}$ for all $1 \le i \le 2n-1$ and all j. In particular, all zeros of $P_i(T)$ lie on the "critical line" $\{s \in \mathbb{C} : \operatorname{Re} s = i/2\}$.

(iv) (Betti numbers) Suppose in addition that X comes from a good reduction of a nonsingular projective variety $\tilde{X}$ over a number field. $X^{\mathrm{an}} = \tilde{X}(\mathbb{C})$ then carries the structure of a complex manifold. And we have $\deg P_i = b_i(X^{\mathrm{an}}), E(X) = \chi(X^{\mathrm{an}})$, where b_i, χ denote the Betti numbers and Euler characteristic in singular homology.

They were proved in full by Deligne [Del74] using the theory of ℓ-adic cohomology developed by Grothendieck [Gro77].

In the case where $X = E$ is an elliptic curve, the proof is classical and can be found e.g. in [Sil09, §V.2] (this treatment makes use of the theory of Tate modules, which can in fact be avoided if one so wishes). It's worth highlighting that Theorem 1.1(iii) for elliptic curves simply comes from Hasse's estimate $|\#E(\mathbb{F}_Q)-(1+Q)| \leq 2\sqrt{Q}$. For curves in general, it follows from a similar estimate:

Theorem 1.2 (Riemann Hypothesis for Curves). *Suppose C is a smooth integral projective curve over $\bar{\mathbb{F}}_p$ of genus g and Q is a power of p, then $|\#C(\mathbb{F}_Q)-(1+Q)| \leq 2g\sqrt{Q}$.*

The purpose of this article is to record a proof of this, originally due to Weil [Wei41], using the theory of intersections on surfaces.

2 Intersections on Surfaces

We'll motivate and construct the intersection pairing on surfaces.

Fix a smooth integral projective surface S over a field k. For starters, we want to understand how closed subvarieties of S intersect each other. Intersections with subvarieties in codimensions 0 (i.e. S) and 2 (i.e. points) feels boring enough to ignore – let's look at curves!

What would be on our wishlist for this theory? Given a pair of curves C, D, we want to produce a number $C \cdot D$ (the "intersection pairing") which can be interpreted as the "number of intersections between C and D". For this to be sensible, if C, D happen to be smooth prime divisors intersecting each other transversely, then $C \cdot D$ should be the naïve number of intersections between them. We also want this intersection pairing to have nice properties, which won't be hard to show once we've guessed the correct definition.

A natural place to start is to write down a working formula for the special case where C, D are integral, smooth and transverse, and see if we can massage it into something that generalises.

The number of intersections between C, D is the degree of the effective divisor on C obtained from restricting D (as a Weil divisor on S). The operation of restricting Weil divisors couldn't be more fiddly in the general case. Nonetheless, we know that (since things are smooth) Weil divisor classes correspond to isomorphism classes of line bundles. And we can always restrict line bundles by pulling it back!

Translating everything into the language of line bundles, we see that the naïve number of intersections between C, D is $\deg_C(\mathcal{O}_S(D) \otimes \mathcal{O}_C)$. And this generalises: Recall that for any line bundle $\mathcal{L}$ on a (not necessarily smooth) projective curve C, its degree is defined as $\deg_C \mathcal{L} = \chi(C, \mathcal{L}) - \chi(C, \mathcal{O}_C)$.

Definition 2.1. For prime divisors C, D on S, their intersection pairing is the integer $C \cdot D = \deg_C(\mathcal{O}_S(D) \otimes \mathcal{O}_C)$. Extending linearly, we make sense of an intersection pairing $\mathrm{Div}(S) \times \mathrm{Div}(S) \to \mathbb{Z}$.

It's not very hard to see that

Proposition 2.1. *The intersection pairing is commutative. Hence it depends only on the Weil divisor classes (therefore descends to a bilinear map $\mathrm{Cl}(S) \times \mathrm{Cl}(S) \to \mathbb{Z}$).*

If we are trying to intersect effective divisors C, D with no shared component, then the pairing simply counts the number of intersections with multiplicity. Here, the multiplicity at a point of intersection p is taken to be the length of $\mathcal{O}_{S,p}/(f,g)$ where f,g are the local equations for C, D respectively.

However, self-intersections can be weird: In general, the intersection pairing is not positive-semidefinite. So the self-intersection $D^2 = D \cdot D$ for a divisor D is actually a very interesting quantity. Before giving an example, let's prove a useful formula for computing these things.

On a smooth projective variety X, we write ω_X, K_X for the canonical bundle and canonical divisor on X, respectively

Proposition 2.2. *If C is a smooth prime divisor on S, then $2g(C) - 2 = C \cdot (C + K_S)$.*

Proof. Take $\deg_C$ on both sides of $\omega_C = \omega_S(C) \otimes \mathcal{O}_C = \mathcal{O}_S(C + K_S) \otimes \mathcal{O}_C$. □

Example 2.1. Fix a smooth integral projective curve C of genus g. Consider $S = C \times C$ and let Δ be the diagonal, which is abstractly isomorphic to C. Let $\mathrm{pr}_1, \mathrm{pr}_2 : S \to C$ be the projections, then $\omega_S = \mathrm{pr}_1^* \omega_C \otimes \mathrm{pr}_2^* \omega_C$. We can write this relation more intuitively as $K_S = \mathrm{pr}_1^* K_C + \mathrm{pr}_2^* K_C$. The proposition then shows that

$$\begin{aligned}\Delta^2 &= 2g - 2 - \Delta \cdot K_S = 2g - 2 - \Delta \cdot (\mathrm{pr}_1^* K_C) - \Delta \cdot (\mathrm{pr}_2^* K_C) \\ &= 2g - 2 - (2g-2) - (2g-2) = 2 - 2g\end{aligned}$$

which is negative for $g > 1$.

This example is a special case of a more general computation.

Proposition 2.3. *Suppose C_1, C_2 are smooth integral projective curves with genera g_1, g_2, respectively. Let $f : C_1 \to C_2$ be a nonconstant morphism and let $\Gamma_f \subset C_1 \times C_2$ be its graph. Then $\Gamma_f^2 = (2 - 2g_2)(\deg f)$.*

Proof. It's essentially the same idea as in the example. Let $S = C_1 \times C_2$ and let $\mathrm{pr}_i : S \to C_i$ be the projections. The formula $K_S = \mathrm{pr}_1^* K_{C_1} + \mathrm{pr}_2^* K_{C_2}$ then shows

$$\begin{aligned}\Gamma_f^2 &= 2g_1 - 2 - \Gamma_f \cdot K_S = 2g_1 - 2 - \Gamma_f \cdot (\mathrm{pr}_1^* K_{C_1}) - \Gamma_f \cdot (\mathrm{pr}_2^* K_{C_2}) \\ &= 2g_1 - 2 - (2g_1 - 2) - (2g_2 - 2)(\deg f) = (2 - 2g_2)(\deg f).\end{aligned}$$ □

3 The Hodge Index Theorem

It wouldn't make much sense to play around with divisors without discussing their Riemann-Roch theory. For a divisor D on S, we write $h^i(D) = \dim_k H^i(S, \mathcal{O}_S(D))$ and $\ell(D) = h^0(D), s(D) = h^1(D)$.

Theorem 3.1 (Riemann-Roch for Surfaces).

$$\ell(D) - s(D) + \ell(K_S - D) = \chi(S, \mathcal{O}_S) + \frac{1}{2} D \cdot (D - K_S).$$

Proof. [Har77, §V.1]. □

Let's use this formula to produce something geometric.

Lemma 3.2. *Suppose* $\ell(D) > 1$, *then* $D \cdot H > 0$ *for any ample* H.

Proof. The condition $\ell(D) > 1$ shows that D is linearly equivalent to a nonzero effective divisor. Since the intersection pairing depends only on the divisor class, we can assume WLOG that D is itself effective and nonzero. The pairing is also bilinear, so WLOG H is very ample.

Thus H is a hyperplane section of S over a certain projective embedding. But all hyperplane sections of a fixed projective embedding are linearly equivalent, so we can replace H with a hyperplane that does not contain a component of D. Then it's clear that $D \cdot H > 0$. □

Theorem 3.3 (Hodge Index Theorem). *Suppose* $D \cdot H = 0$ *with* H *ample, then* $D^2 \leq 0$.

Remark. In the case where $D^2 = 0$, we in fact have $D \cdot C = 0$ for all divisor C. This will not be used for our purpose.

Proof. In view of the preceding lemma, it suffices to show that if D is a divisor with $D^2 > 0$ then there is some $m \in \mathbb{Z}$ with $\ell(mD) > 1$.

By Theorem 3.1, $\ell(mD) + \ell(K_S - mD)$ is bounded below by the quadratic polynomial $(D^2/2)m^2 - ((D \cdot K_S)/2)m + \chi(S, \mathcal{O}_S)$. It has positive leading coefficient, so we know that for any $m_0 > 0$ there is some $m > 0$ with $\ell(\pm mD) + \ell(K_S \mp mD) \geq m_0 + 1$.

If either $\ell(mD) > 1$ or $\ell(-mD) > 1$ then we are done. Otherwise $\ell(\pm mD) \leq 1$, so $\ell(K_S \mp mD) \geq m_0$. In particular, $\ell(K_S + mD) > 0$ and hence $K_S + mD$ is linearly equivalent to an effective divisor. Therefore $\ell(2K_S) = \ell(K_S + mD + K_S - mD) \geq \ell(K_S - mD) \geq m_0$. But this is absurd since $m_0 > 0$ is arbitrary. □

Let's return to our example where S is the product $C_1 \times C_2$ of smooth integral projective curves. Choose any points $c_1 \in C_1, c_2 \in C_2$ and let $D_1 = C_1 \times c_2$ and $D_2 = c_1 \times C_2$.

Theorem 3.4 (Castelnuovo-Severi). $D^2 \leq 2(D \cdot D_1)(D \cdot D_2)$ *for any divisor* D *on* S.

Proof. $H = D_1 + D_2$ is ample. Indeed, c_i is ample on C_i, so we can choose $m_i > 0$ such that $m_i c_i$ is very ample on C_i. Suppose $\phi_i : C_i \to \mathbb{P}^{n_i}$ are the projective embeddings associated to $m_i c_i$. Then $\mathcal{O}_S(m_1 m_2 H) = (\phi_1 \times \phi_2)^*(\pi_1^* \mathcal{O}_{\mathbb{P}^{n_1}}(m_2) \otimes \pi_2^* \mathcal{O}_{\mathbb{P}^{n_2}}(m_1))$ where $\pi_i : \mathbb{P}^{n_1} \times \mathbb{P}^{n_2} \to \mathbb{P}^{n_i}$ are the projections.

But $\phi_1 \times \phi_2$ is a closed embedding and $\pi_1^* \mathcal{O}_{\mathbb{P}^{n_1}}(m_2) \otimes \pi_2^* \mathcal{O}_{\mathbb{P}^{n_2}}(m_1)$ is very ample, so $m_1 m_2 H$ must be very ample. This means that H is ample.

Now let $E = D - (D \cdot D_2)D_1 - (D \cdot D_1)D_2$. It's clear that $D_1 \cdot D_2 = 1$. We also have $D_1^2 = D_2^2 = 0$, for example by Proposition 2.2. Therefore $E \cdot H = 0$. Theorem 3.3 then imples that $E^2 \leq 0$, which expands to give the desired inequality. □

4 Riemann Hypothesis for Curves

How are all these geometry of intersections related to point-counting? Observe the following: Fix a prime p and a power Q of it. The finite field $\mathbb{F}_Q$ is the set of fixed points of the Q-Frobenius $\mathrm{Fr}_Q : \bar{\mathbb{F}}_p \to \bar{\mathbb{F}}_p$. Similarly, for a smooth integral projective curve C over $\bar{\mathbb{F}}_p$, $C(\mathbb{F}_Q)$ is the set of fixed $\bar{\mathbb{F}}_p$-points of the geometric Frobenius $\mathrm{Fr}_Q : C \to C$.

So the point-counting problem is actually a fixed-point problem. But fixed-point problems are naturally related to intersection problems. In the context of sets, fixed points of a function $f : A \to A$ are exactly the intersections between the graph of f and the diagonal in $A \times A$!

This idea is not hard to make precise: Let $\Gamma \subset S = C \times C$ be the graph of Fr_Q, then $\Gamma \neq \Delta$ and they are both irreducible, so they share no component. Furthermore, the multiplicities at the intersections are all 1 (exercise), so $\Gamma \cdot \Delta = \#C(\mathbb{F}_Q)$. The problem is now a matter of how to estimate the value of this intersection. Denote it by N.

Recall that we've computed in Proposition 2.3 that $\Gamma^2 = (2-2g)Q$ and $\Delta^2 = 2-2g$. So Theorem 3.4 applied to $D = r\Gamma + s\Delta$ gives

$$(2-2g)Qr^2 + 2Nrs + (2-2g)s^2 \leq 2(Qr+s)(r+s)$$

which simplifies to $0 \leq gQr^2 + (Q+1-N)rs + gs^2$. Thus $gQx^2 + (Q+1-N)x + g \geq 0$ for any $x \in \mathbb{Q}$, hence for any $x \in \mathbb{R}$. So $(Q+1-N)^2 - 4g^2Q \leq 0$. This rearranges to $|N-(1+Q)| \leq 2g\sqrt{Q}$, which is Theorem 1.2.

References

[Del74] Pierre Deligne. La conjecture de Weil : I. *Publications Mathématiques de l'IHÉS*, 43:273–307, 1974.

[Gro77] Alexandre Grothendieck. *Séminaire de géométrie algébrique du Bois-Marie 1965–66, Cohomologie ℓ-adique et fonctions L, SGA5*, volume 589 of *Springer Lecture Notes*. Springer-Verlag, 1977.

[Har77] Robin Hartshorne. *Algebraic Geometry*, volume 52 of *Graduate Texts in Mathematics*. Springer, 1977.

[Sil09] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, 2009.

[Wei41] André Weil. On the Riemann hypothesis in function-fields. *Proceedings of the National Academy of Sciences*, 27(7):345–347, 1941.