The Weil Conjectures for Curves

Caleb Ji

Summer 2021

1 Introduction

We will explain Weil's proof of his famous conjectures for curves. For the Riemann hypothesis, we will follow Grothendieck's argument [1]. The main tools used in these proofs are basic results in algebraic geometry: Riemann-Roch, intersection theory on a surface, and the Hodge index theorem.

For references: in Section 2 we used [3], while the rest can be found in Hartshorne [2] V.1 and Appendix C (some of it in the form of exercises).

1.1 Statements of the Weil conjectures

We recall the statements. 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 $\mathbb{F}_{q^r}$.

Theorem 1.1 (Weil conjectures)**.** *Use the above notation.*

1. *(Rationality) $Z(X,t)$ is a rational function of t.*
2. *(Functional equation) Let E be the Euler characteristic of X considered over $\mathbb{C}$. Then*
$$Z\left(\frac{1}{q^n t}\right) = \pm q^{nE/2} t^E Z(t).$$
3. *(Riemann hypothesis) We can write*
$$Z(t) = \frac{P_1(t)\cdots P_{2n-1}(t)}{P_0(t)\cdots P_{2n}(t)}$$
where $P_0(t) = 1-t, P_{2n}(t) = 1-q^n t$ and all the $P_i(t)$ are integer polynomials that can be written as
$$P_i(t) = \prod_j (1-\alpha_{ij}t).$$
Finally, $|\alpha_{ij}| = q^{i/2}$.
4. *(Betti numbers) The degree of the polynomials P_i are the Betti numbers of X considered over $\mathbb{C}$.*

Note that $\frac{d}{dt}\log Z(X,t) = \sum_{r=0}^{\infty} N_{r+1}t^r$. Then with some elementary manipulation, we can connect this zeta function with a possibly more familiar-looking 'arithmetic zeta function':

$$Z(X, q^{-s}) = \zeta_X(s) := \prod_x \frac{1}{1 - N(x)^{-s}},$$

where the product ranges over all closed points $x \in X$, and $N(x)$ is the magnitude of the residue field of x. Under this interpretation, we see that the Riemann hypothesis states that the roots of $\zeta_X(s)$ have real part $\frac{1}{2}, \frac{3}{2}, \cdots, \frac{2n-1}{2}$.

1.2 Approaches

As is well-known, all the Weil conjectures with the exception of the Riemann hypothesis can be explained through Grothendieck's construction of the étale cohomology of schemes. The Riemann hypothesis was proven by Deligne, who incorporated certain analytical tools into his proof. Now there are multiple proofs. In the case of curves, there is also a more elementary proof due to Bombieri. Nevertheless, the proof we follow is instructive because it illustrates the use of fundamental results in algebraic geometry. However, it does not consider the action of the Frobenius morphism, which is at the heart of the approach through étale cohomology. Combining these perspectives (along with much deeper considerations, for sure), Grothendieck was led to the standard conjectures, from which the Riemann hypothesis (for all varieties) would follow as a corollary. These are still open.

2 Rationality, functional equation, and Betti numbers

2.1 Rationality and Betti numbers

To prove the rationality of the zeta function of a curve, we will need the following results from algebraic geometry.

Theorem 2.1 (Riemann-Roch). *Let X be a smooth projective curve over k of genus g with canonical divisor K. Then for any divisor D, we have*

$$l(D) - l(K - D) = \deg D - g + 1.$$

Proposition 2.2. *[[2], Prop. II.7.7] Let D be a divisor of X. Then the set of effective divisors of X linearly equivalent to D may be identified with the set $\{H^0(X, L(D))\backslash 0\}/k^*$ in the following way.*

Take $0 \neq s \in H^0(X, L(D))$ and let (U_i, ϕ_i) be trivializations of $L(D)$. Then define the associated Cartier divisor $(s)_0 = \{(U_i, \phi_i(s))\}$.

Now we attack rationality. We have

$$Z(X, q^{-s}) = \prod_x \frac{1}{1 - N(x)^{-s}} \Rightarrow Z(X,t) = \prod_{r=1}^{\infty}(1 - t^r)^{M_r},$$

where M_r is the number of closed points $x \in X$ with residue field $\mathbb{F}_{q^r}$. Expanding this, we see that $Z(X,t)$ is nothing other than the generating function of the number of effective divisors of degree r. (!) Let us denote this sequence by A_r.

By Proposition 2.2, the number of effective divisors linearly equivalent to a fixed D is equal to $\frac{q^{l(D)}-1}{q-1}$. The key point is that by Riemann-Roch, for $\deg D > 2g - 2$, this number is explicitly computable. Namely, in this case $l(D) = \deg D - g + 1$. Moreover, the number of distinct linear equivalence classes is given by $|\operatorname{Cl}^0(X)|$, since in this range every divisor is linearly equivalent to an effective one[1]. Thus, we may break the zeta function into two parts: $Z(X,t) = Z_1(X,t) + Z_2(X,t)$ with

$$Z_1(X,t) = \sum_{r=0}^{2g-2} A_r t^r$$

and

$$Z_2(X,t) = \sum_{r>2g-2} A_r t^r = |\operatorname{Cl}^0(X)| \sum_{r>2g-2} \frac{q^{r-g+1}-1}{q-1} t^r = \frac{|\operatorname{Cl}^0(X)|}{q-1} \cdot \frac{(q^g-1)t^{2g-1} + (q-q^g)t^{2g}}{(1-t)(1-qt)}.$$

Summing $Z_1(X,t)$ and $Z_2(X,t)$ yields the rationality statement. Moreover, the coefficients of the numerator and denominator are integers. By analyzing the numerator and showing it has degree $2g$, we will obtain the statement for the Betti numbers.

First, note that $A_0 = 1$; this ensures that the numerator has constant term 1. As for the coefficient of t^{2g}, note that the canonical divisor contributes via $l(K) = g$, and all D of degree $2g-2$ contribute via $l(D) = g-1$. Thus,

$$A_{2g-2} = \frac{|\operatorname{Cl}^0(X)|}{q-1}(q^{g-1}-1) + q^{g-1}.$$

This gives that the coefficient of t^{2g} in the numerator is precisely $q^g \neq 0$. In fact, this shows that we can write

$$Z(X,t) = \frac{\prod_{i=1}^{2g}(1-\alpha_i t)}{(1-t)(1-qt)}$$

where the α_i are algebraic integers that come in conjugate pairs, and moreover $\prod_{i=1}^{2g} \alpha_i = q^g$.

2.2 Functional equation

We would like to show that

$$Z(X, \frac{1}{qt}) = q^{1-g} t^{2-2g} Z(X,t).$$

The idea will be to split $Z(X,t)$ into two summands for which we can verify this equality. These will not quite be the Z_1 and Z_2 above. Indeed, if we want to compare $Z_2(X,t)$ and $Z_2(X, \frac{1}{qt})$, note that there is a $|\operatorname{Cl}^0(X)|$ factor which does not show up with Z_1. Note that this term appears as long as $\deg D \geq g$, so that all these D are linearly equivalent to effective ones. Thus, instead of starting from $2g-1$, we start from g. We set

$$Z_4(X,t) = |\operatorname{Cl}^0(X)| \sum_{\deg D \geq g} \frac{q^{\deg D - g+1}-1}{q-1} t^{\deg D} = |\operatorname{Cl}^0(X)| \frac{t^g}{(1-t)(1-qt)}.$$

Here, as below, we are really summing over linear equivalence classes of divisors. We get

$$q^{g-1}t^{2g-2} Z_4(X, \frac{1}{qt}) = |\operatorname{Cl}^0(X)| q^{g-1} t^{2g-2} \frac{(qt)^{-g}}{(1-(qt)^{-1})(1-t^{-1})} = |\operatorname{Cl}^0(X)| \frac{t^g}{(1-t)(1-qt)},$$

so $Z_4(X,t) = q^{g-1}t^{2g-2} Z_4(X, \frac{1}{qt})$.

[1] Technically, we are assuming $g > 0$ for everything to make sense, which is of course harmless.

What remains? We set

$$Z_3(X,t) = Z(X,t) - Z_4(X,t) = Z_1(X,t) - \sum_{\deg D=g}^{2g-2} \frac{q^{\deg D+1-g}-1}{q-1} t^{\deg D}.$$

We wish to verify the functional equation for Z_3. This is basically just a computation. The main insight is to consider the involution of divisors of degrees from 0 through $2g-2$ defined by $D \mapsto K-D$. Note that we can really consider all such D when considering their contribution to $Z(X,t)$, because those that are not effective will contribute $\frac{q^0-1}{q-1}t^r = 0$. We begin the computation by recalling that

$$Z_1(X,t) = \sum_{\deg D=0}^{2g-2} \frac{q^{l(D)}-1}{q-1} t^{\deg D}.$$

On the other hand, 'what we want' is

$$q^{g-1}t^{2g-2}Z_1(\frac{1}{qt}) = \sum_{\deg D=0}^{2g-2} \frac{q^{l(K-D)} - q^{l(K-D)-l(D)}}{q-1} t^{2g-2-\deg D} = \sum_{\deg D=0}^{2g-2} \frac{q^{l(D)} - q^{l(D)-l(K-D)}}{q-1} t^{\deg D}.$$

by applying the involution in the last step. It simply remains to do the computation for the extra piece of $Z_3(X,t)$ and verify that the differences cancel out. This is indeed the case through another application of the involution. We leave this last calculation to the reader[2].

3 Intersection theory on a surface

The proof of the Riemann hypothesis for curves that we will explain involves studying the self-intersection number of the graph of the Frobenius morphism. To understand it, we will begin by building up basic intersection theory on a surface. In general, intersection theory is (to put it mildly) a very intricate affair. But many simplifications occur in the case of curves on surfaces, which makes this job not too difficult.

3.1 Definitions

By surface, we refer to a smooth projective variety of dimension 2 over an algebraically closed field k. By a curve on a surface, we mean an effective divisor on the surface. We say that two curves C and D meet transversely if, for every common point P, their local defining equations f, g generate the maximal ideal of the local ring $\mathcal{O}_{P,X}$.

We would like to determine an intersection pairing $\mathrm{Div}\, X \times \mathrm{Div}\, X \to \mathbb{Z}$ that expresses the intersection number of two curves on a surface. Naturally, if C and D are nonsingular and meet transversely at d points, their intersection number should be $C \cdot D = d$. One may want to extend this to any two curves that do not share a common component by defining the intersection multiplicity at a common point P to be the length of $\mathcal{O}_{P,X}/(f,g)$. This does indeed work, but here are two good reasons not to take it as a definition. First, there is no clear way to extend this to self-intersections, whereas in reality this notion exists and is important! Second, this is not a priori a good definition, because one has not checked that it fulfills the basic axioms we would like to impose on the intersection number. In fact, the obvious generalization of this definition to higher dimensions is wrong! One must account for higher Tors, as in Serre's Tor

[2]One might be skeptical because applying the involution beginning from $\deg D = g$ 'misses' the case $\deg D = g-1$. But note that in this case, the difference coming from Z_1 is also 0. (!)

formula.

Instead, we would like to impose the following axioms.

1. If nonsingular C, D meet transversely at d points, then $C \cdot D = d$.
2. $C \cdot D = D \cdot C$.
3. $(C_1 + C_2) \cdot D = C_1 \cdot D + C_2 \cdot D$.
4. The intersection pairing depends only on the linear equivalence class of the curves.

The uniqueness of the pairing works in the following way. Let C and D be any divisors; we wish to use the axioms to express $C\dot{D}$ in terms of intersection numbers of transverse nonsingular curves. First, fix a very ample divisor H on X such that $C + H$ and $D + H$ are also very ample. By Bertini's theorem, almost all curves in the complete linear system of a very ample divisor are nonsingular meet any finite number of irreducible curves transversely. Then we can choose mutually transverse nonsingular curves $C' \in |C + H|, D' \in |D + H|, E', F' \in |H|$. Then we are forced to have $C \cdot D = (C' - E') \cdot (D' - F')$, which is determined.

Next, to show this is well-defined, we must show this construction is independent of choices. Since we can express every divisor as a difference of two very ample ones, it suffices to check this restricted to very ample divisors. That is, given C and D very ample, we need to show that $C' \cdot D' = C' \cdot D''$ where $C' \in |C|$ is nonsingular and we choose $D', D'' \in |D|$ nonsingular and transverse to C'. This follows from the following proposition.

Proposition 3.1. *Let C be an irreducible nonsingular curve on X and let D be a curve meeting C transversely. Then*

$$|C \cap D| = \deg_C(L(D) \otimes \mathcal{O}_C).$$

Proof. Tensoring the exact sequence

$$0 \to L(-D) \to \mathcal{O}_X \to \mathcal{O}_D \to 0$$

with $\mathcal{O}_C$, we obtain an exact sequence

$$0 \to L(-D) \otimes \mathcal{O}_C \to \mathcal{O}_C \to \mathcal{O}_{C\cap D} \to 0.$$

Then $L(D)\otimes\mathcal{O}_C$ corresponds to the divisor $\mathcal{O}_{C\cap D}$ on C, whose degree is simply $|C\cap D|$ because C and D meet transversely. □

Now that we have constructed the intersection pairing, we can analyze local intersection multiplicities and self-intersection numbers.

Proposition 3.2. *Let C and D be curves on X with no common irreducible component. For each $P \in C \cap D$, define $(C \cdot D)_P = \operatorname{len} \mathcal{O}_{P,X}/(f, g)$. Then*

$$C \cdot D = \sum_{P\in C\cap D} (C \cdot D)_P.$$

Proof. Note that $\dim_k H^0(X, \mathcal{O}_{C\cap D}) = \sum_{P\in C\cap D}(C \cdot D)_P$. Then using additivity of the Euler characteristic in

$$0 \to L(-D) \otimes \mathcal{O}_C \to \mathcal{O}_C \to \mathcal{O}_{C\cap D} \to 0,$$

we get

$$\sum_{P\in C\cap D} (C \cdot D)_P = \chi(\mathcal{O}_C) - \chi(L(-D) \otimes \mathcal{O}_C).$$

Note that if C and D did intersect transversely, this would be the correct formula. We also see that this value only depends on the linear equivalence class of D, and therefore C as well. Therefore we may replace C and D with differences of transverse nonsingular curves, which will give the desired intersection number $C \cdot D$. □

Now define the self intersection number $C^2 = C \cdot C$.

Proposition 3.3. *The self-intersection number is given by*

$$C^2 = \deg_C N_{C/X},$$

where $N_{C/X} = \mathcal{H}om(I/I^2, \mathcal{O}_C)$ is the normal sheaf.

Proof. By definition, we have $C^2 = \deg_C(L(C) \otimes \mathcal{O}_C)$. The dual of this sheaf, $L(-C) \otimes \mathcal{O}_C$, is isomorphic to I/I^2. The result follows. □

Example 3.4. *Let C be a curve of genus g and consider the diagonal $\Gamma \in C \times_k C$. Then $N_{\Gamma/C\times C}$ is the dual of the pullback of the ideal sheaf $\Delta^*(I/I^2)$, which is none other than the sheaf of differentials. This coincides with the canonical sheaf, which has degree $2g-2$. Thus $\Gamma^2 = 2-2g$.*

3.2 Riemann-Roch for surfaces

First let us prove the adjunction formula.

Theorem 3.5 (Adjunction Formula)**.** *Let $Y \subset X$ be a smooth subvariety of codimension r of a smooth variety. Then*

$$\omega_Y \cong \omega_X \otimes \wedge^r N_{Y/X}.$$

If $r = 1$, then

$$\omega_Y \cong \omega_X \otimes L(Y) \otimes \mathcal{O}_Y.$$

Proof. Begin with the exact sequence

$$0 \to I/I^2 \to \Omega_X \otimes \mathcal{O}_Y \to \Omega_Y \to 0.$$

Taking highest exterior powers, we get $\omega_X \otimes \mathcal{O}_Y \cong \wedge^r(I/I^2) \otimes \omega_Y \Rightarrow \omega_Y \cong \omega_X \otimes \wedge^r N_{Y/X}$, as desired.

If $r = 1$, then $N_{Y/X} \cong (I/I^2)^\vee \cong (L(-Y) \otimes \mathcal{O}_Y)^{-1}) \cong L(Y) \otimes \mathcal{O}_Y$, and the result follows. □

Corollary 3.6 (adjunction formula)**.** *Let C be a nonsingular curve of genus g on the surface X, which has canonical divisor K. Then*

$$2g-2 = C \cdot (C+K).$$

Proof. Taking degrees in the adjunction formula above, we have $2g-2 = \deg \omega_C = \deg(\omega_X \otimes L(C) \otimes \mathcal{O}_C)$. Viewing $\omega_X \otimes L(C)$ as a curve on X, we get that the RHS is just $C \cdot (C+K)$. □

We now wish to prove the following theorem.

Theorem 3.7 (Riemann-Roch for surfaces)**.** *Let D be a divisor on a surface X. Then*

$$l(D) - \dim H^1_k(X, L(D)) + l(K-D) = \chi(L(D)) = \frac{1}{2} D \cdot (D-K) + \chi(\mathcal{O}_X).$$

Proof. The first equality is just Serre duality. As usual, write $D = C - E$ where C and E are nonsingular. Considering the exact sequences

$$0 \to L(C-E) \to L(C) \to L(C) \otimes \mathcal{O}_E \to 0$$
$$0 \to \mathcal{O}_X \to L(C) \to L(C) \otimes \mathcal{O}_C \to 0,$$

we obtain $\chi(L(D)) = \chi(\mathcal{O}_X) + \chi(L(C) \otimes \mathcal{O}_C) - \chi(L(C) \otimes \mathcal{O}_E)$. We can compute the last two terms using Riemann-Roch for curves on C and E. We have

$$\chi(L(C) \otimes \mathcal{O}_C) = \deg(L(C) \otimes \mathcal{O}_C) - g_C + 1.$$

By the adjunction formula, $g_C = \frac{1}{2} C \cdot (C + K) + 1$. Doing the same computation for the other term, we put it all together and obtain the desired result. □

3.3 Hodge index theorem

Let H be a very ample divisor on a surface X. Then for a curve C on X, the degree of C under the embedding given by H into $\mathbb{P}^n$ coincides with $C \cdot H$. Indeed, recall that the degree of C is defined as the linear coefficient of the Hilbert polynomial, which is given by the Euler characteristic of $\chi(\mathcal{O}_C(n))$. As usual we can reduce to the case of C and H and C having no common irreducible component. Then as before we can show that the intersection number is given by $\chi(\mathcal{O}_C) - \chi(L(-H) \otimes \mathcal{O}_C) = \chi(\mathcal{O}_C) - \chi(\mathcal{O}_C(-1))$, which is the desired coefficient. In particular, $C \cdot H$ is positive. This fact holds for ample H, since a positive multiple of an ample divisor is very ample. Then we see that if $C \cdot H > K \cdot H$, then $(K - C) \cdot H < 0$ so no linear equivalence class of $K - C$ can be effective. Then $l(K - D)$, so by Serre duality, $H^2(X, L(D)) = 0$.

We use this to prove the following lemma which will be used in the proof of the Hodge Index Theorem.

Lemma 3.8. *Let H be an ample divisor on X, and let D be a divisor such that $D \cdot H > 0$ and $D^2 > 0$. Then for all $n >> 0$, nD is linearly equivalent to an effective divisor.*

Proof. By the previous result and the Riemann-Roch theorem, we have

$$l(nD) \geq \frac{1}{2}(nD) \cdot (nD - K) + \chi(\mathcal{O}_X)$$

for $n >> 0$. This is clearly positive for n sufficiently large. □

Theorem 3.9 (Hodge Index Theorem). *Let H be an ample divisor on the surface X and let D be a nonzero divisor with $D \cdot H = 0$. Then $D^2 < 0$.*

Proof. Otherwise, first consider the case $D^2 > 0$. We have that $D + nH$ is ample for some sufficiently large n. Then $D \cdot (D + nH) = D^2 > 0$, so by the previous lemma mD is linearly equivalent to an effective divisor for $m >> 0$. This contradicts the fact that $D \cdot H = 0$.

Now say $D^2 = 0$. Since $D \neq 0$, there is some E with $D \cdot E \neq 0$. Let $E' = (H^2)E - (E \cdot H)H$. Then $D \cdot E' \neq 0$ and $E' \cdot H = 0$. Then for sufficiently large n, we have $(nD + E')^2 > 0$ and $(nD + E') \cdot H = 0$. But this is impossible by the previous argument. □

Finally, we state the Nakai-Moishezon criterion for ampleness.

Theorem 3.10 (Nakai-Moishezon criterion). *A divisor D on a surface X is ample if and only if $D^2 > 0$ and $D \cdot C > 0$ for all irreducible curves C in X.*

For a proof, see [2], V.1.10.

4 Riemann hypothesis for curves

The proof of the Riemann hypothesis for curves rests on the Hasse-Weil bound, which states that

$$N := |C(\mathbb{F}_q)| = q + 1 - a \qquad \text{where } |a| \leq 2g\sqrt{q}.$$

This 'square-root error term' bound easily implies the Riemann hypothesis using the functional equation, similar to the case of the Riemann zeta function. We will use the intersection theory developed in the previous section to prove the Hasse-Weil bound.

4.1 Proof of the Hasse-Weil bound

The idea is to use intersection theory of the diagonal Δ and the graph of the Frobenius Γ on the surface $C \times_{\overline{\mathbb{F}_q}} C$. Note that we are taking C over $\overline{\mathbb{F}_q}$; we will henceforth drop the subscript in the product. Let us compute the pairwise intersection numbers. First, we have already seen that

$$\Delta^2 = 2 - 2g.$$

Next, it is intuitively true that $\Delta \cdot \Gamma = N$, because the points fixed by the Frobenius are precisely the ones defined over $\mathbb{F}_q$. However, we ought to check that these points are unreduced to ensure that this count gives the correct intersection number. It suffices to check this on affine space. This is just saying that

$$\prod_{i=1}^{k} \operatorname{Spec} \mathbb{F}_q[x_i]/(x_i^q - x_i)$$

is reduced, which is clear by taking derivatives. Thus $\Delta \cdot \Gamma = N$.

Finally, we compute Γ^2. To do this, note that Γ is the pullback of Δ under the Frobenius. We also have that, in general, $f_* f^*$ is multiplication by $\deg f$ on divisors, and f_*, f^* are adjoint with respect to intersection product. Setting f to be the Frobenius, this gives

$$\Gamma^2 = (f^*\Delta, f^*\Delta) = (f_* f^*\Delta, \Delta) = q\Delta^2 = q(2-2g).$$

Alternatively, we may use the adjunction formula. This gives

$$2g - 2 = \Gamma^2 + \Gamma \cdot K_{C \times C}.$$

We can express $K_{C \cdot C}$ as the sum of the pullbacks $p_1^* \cdot K_C + p_2^* K_C$. Now note that Γ intersects $C \times \mathrm{pt}$ and $\mathrm{pt} \times C$ with multiplicity 1 and q. Since $\deg K_C = 2g - 2$, this gives $\gamma^2 = 2g - 2 - (q+1)(2g-2) = q(2-2g)$, as desired.

We will now relate this intersection numbers by means of a general inequality that apparently goes all the way back to the classical Italian school. Apparently, Grothendieck [1], following Mattuck-Tate, simplified the proof through the Hodge index theorem and the Nakai-Moishezon criterion.

Theorem 4.1. *Let $X = C \times C'$ and let $l = C \times \mathrm{pt}, m = \mathrm{pt} \times C$. If D is a divisor on X such that $D \cdot l = a$ and $D \cdot m = b$, then*

$$D^2 \leq 2ab.$$

Proof. First, we claim that if H is ample, we have $(D^2)(H^2) \leq (D \cdot H)^2$ for any D. Indeed, apply the Hodge index theorem to $E = (H^2)D - (H \cdot D)H$.

Next, let $H = l + m, E = l - m$. By the Nakai-Moishezon criterion, H is ample. Then apply the previous result to the divisor

$$(H^2)(E^2)D - (E^2)(D \cdot H)H - (H^2)(D \cdot E)E.$$

Expanding this gives precisely $D^2 \leq 2ab$. $\square$

We now conclude the proof of the Hasse-Weil bound by applying the previous inequality to $D = r\Gamma + s\Delta$ for $r, s \in \mathbb{Z}$. We have $D \cdot l = rq + s$ and $D \cdot m = r + s$. Expanding, we get

$$(r^2 q + s^2)(2 - 2g) + 2rsN \leq 2(rq + s)(r + s).$$

Simplifying, we get

$$|N - q - 1| \leq \left| \frac{rq}{s} + \frac{sg}{r} \right|,$$

where the absolute values comes from whether rs is positive or negative. Finally, we note that the RHS can be made arbitrarily close to $2g\sqrt{q}$, so we are done.

4.2 Completion of the proof

We have now shown that $|N - q - 1| \leq 2g\sqrt{q}$. Doing this for each $\mathbb{F}_{q^r}$, we have that $a_r := |N_r - q^r - 1| \leq 2g\sqrt{q^r}$. Previously, we showed we can write the zeta function as

$$Z(X, t) = \frac{\prod_{i=1}^{2g}(1 - \alpha_i t)}{(1 - t)(1 - qt)}$$

where the α_i are algebraic integers that come in conjugate pairs, and moreover $\prod_{i=1}^{2g} \alpha_i = q^g$. The goal now is to show that $|\alpha_i| = \sqrt{q}$. Since we know $\prod_{i=1}^{2g} \alpha_i = q^g$, it is enough to show that $|\alpha_i| \leq \sqrt{q}$.

We must relate a_r to the α_i. This is not terribly difficult, as we can compute

$$\begin{aligned}
\sum_{r \geq 1} N_r t^{r-1} = \frac{d}{dt} \log(Z(X, t)) &= \frac{d}{dt} \log \frac{\prod_{i=1}^{2g}(1 - \alpha_i t)}{(1 - t)(1 - qt)} \\
&= \sum_{i=1}^{2g} \frac{-\alpha_i}{1 - \alpha_i t} + \frac{1}{1 - t} + \frac{q}{1 - qt} \\
&= \sum_{r \geq 1} (q^r + 1 - \sum_{i=1}^{2g} \alpha_i^r) t^{r-1}.
\end{aligned}$$

Thus, we have $a_r = \sum_{i=1}^{2g} \alpha_i^r$. We have to use the fact that $|a_r| \leq 2gq^{r/2}$ to show that each α_i has absolute value at most $q^{1/2}$. To do this, assume for sake of contradiction that $|alpha_1| > q^{1/2}$ with $|\alpha_1|$ maximal and write

$$\sum_{r \geq 1} a_r t^r = \sum \frac{\alpha_i t}{1 - \alpha_i t}.$$

Then as $t \to \alpha_1^{-1}$, the LHS converges while the RHS diverges, contradiction. Thus, $|\alpha_i| \leq q^{1/2} \Rightarrow |\alpha_i| = q^{1/2}$, as desired.

References

[1] Alexander Grothendieck. *Sur une note de Mattuck-Tate*, J. Reine u. Angew. Math. 200 (1958), 208–215.

[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