LECTURE 4. THE WEIL CONJECTURES FOR CURVES

In this lecture we consider a smooth projective curve X defined over $k = \mathbf{F}_q$. Let $\overline{k}$ denote an algebraic closure of k and $\overline{X} = X \times_{\operatorname{Spec} k} \operatorname{Spec} \overline{k}$. If $\pi\colon \overline{X} \to X$ is the natural projection, then for every quasicoherent sheaf $\mathcal{F}$ on X, we have canonical isomorphisms $H^i(X, \mathcal{F}) \otimes_k \overline{k} \simeq H^i(\overline{X}, \pi^*(\mathcal{F}))$.

We always assume that X is geometrically connected, that is, $\overline{X}$ is connected. In this case $\overline{X}$ is a smooth, irreducible, projective curve over $\overline{k}$. Since $H^0(\overline{X}, \mathcal{O}_{\overline{X}}) = \overline{k}$, we get $H^0(X, \mathcal{O}_X) = k$. Recall that the *genus* of X is $g := h^1(X, \mathcal{O}_X) = h^1(\overline{X}, \mathcal{O}_{\overline{X}})$.

Our goal in this lecture is to prove the Weil conjectures in this setting. As we have seen in Lecture 2, $Z(X, t)$ can be viewed as a generating function for effective 0-cycles on X. Since X is a curve, a 0-cycle is the same as a Weil divisor on X. We start by recalling a few generalities about divisors and line bundles on X.

A divisor on X is a finite formal combination $\sum_{i=1}^r a_i P_i$, where $a_i \in \mathbf{Z}$ and P_i is a closed point of X. One says that D is effective if $a_i \geq 0$ for all i. Note that every such divisor is automatically Cartier since X is nonsingular. The *degree* of D is $\deg(D) := \sum_i a_i \cdot [k(P_i) : k]$. The line bundle associated to D is denoted by $\mathcal{O}_X(D)$. The degree map induces a morphism of abelian groups $\deg\colon \operatorname{Pic}(X) \to \mathbf{Z}$.

Given a line bundle L on X, the set of effective divisors D on X with $\mathcal{O}_X(D) \simeq L$ is in bijection with the quotient of $H^0(X, L) \smallsetminus \{0\}$ by the action of the invertible elements in $H^0(X, \mathcal{O}_X)$ via multiplication. By assumption, $H^0(X, \mathcal{O}_X) = k$, hence this space of divisors is nonempty if and only if $H^0(X, L) \neq 0$, and in this case it is in bijection with $\mathbf{P}^{h^0(L)-1}(\mathbf{F}_q)$, hence it has $\frac{q^{h^0(L)}-1}{q-1}$ elements.

The Riemann-Roch theorem says that for every divisor D on X,

$$\chi(X, \mathcal{O}_X(D)) = \deg(D) - g + 1. \tag{1}$$

Furthermore, recall that if $\deg(\mathcal{O}_X(D)) \geq 2g - 1$, then $H^1(X, \mathcal{O}_X(D)) = 0$, in which case $h^0(X, \mathcal{O}_X(D)) = \deg(D) - g + 1$. We will also make use of Serre duality: if $\omega_X = \Omega_{X/k}$ is the canonical line bundle on X, then for every line bundle L on X we have $h^1(X, L) = h^0(X, \omega_X \otimes L^{-1})$. Note that $\deg(\omega_X) = 2g - 2$. All the above assertions can be proved by passing to $\overline{k}$, and using the familiar results over algebraically closed fields, see [Har, Chapter IV.1].

There is a variety $J(X)$ defined over k, with the following property: for every field extension k' of k, the k'-valued points of $J(X)$ are in natural bijection with the line bundles of degree zero on $X \times_{\operatorname{Spec} k} \operatorname{Spec} k'$. In particular, the number h of line bundles on X of degree zero is equal to $|J(X)(k)|$, hence it is finite (and, of course, positive). Note that if $\operatorname{Pic}^m(X)$ denotes the set of line bundles on X of degree m, then $\operatorname{Pic}^m(X)$ is either empty, or it has h elements (we will see below that $\operatorname{Pic}^m(X)$ is never empty).

1. Rationality of the zeta function

We first prove the first of the Weil conjectures. In fact, we will prove the following more precise statement below. In this section and the next one, we follow [Lor, Chapter 8].

Theorem 1.1. *If X is a smooth, geometrically connected, projective curve of genus g over $\mathbf{F}_q$, then*

$$Z(X,t) = \frac{f(t)}{(1-t)(1-qt)},$$

where $f \in \mathbf{Z}[t]$ is a polynomial of degree $\leq 2g$, with $f(0) = 1$ and $f(1) = h$, where $h = |J(X)(\mathbf{F}_q)|$.

Proof. It follows from Proposition 1 in Lecture 2 that

$$Z(X,t) = \prod_{x \in X_{\mathrm{cl}}} \frac{1}{1-t^{\deg(x)}} = \sum_{D \geq 0} t^{\deg(D)},$$

where the last sum is over the effective divisors D on X. We will break this sum into two sums, depending on whether $\deg(D) \geq 2g-1$ or $\deg(D) \leq 2g-2$.

Let $e > 0$ be the positive integer such that $\deg(\mathrm{Pic}(X)) = e\mathbf{Z}$. For every m such that $e|m$, we have

$$|\{L \in \mathrm{Pic}(X) \mid \deg(L) = m\}| = h.$$

As we have seen, if $h^0(X,L) \geq 1$, then the number of effective divisors D with $\mathcal{O}_X(D) \simeq L$ is $\frac{q^{h^0(L)}-1}{q-1}$. In particular, if m is a nonegative integer with $m \geq 2g-1$, then for every $L \in \mathrm{Pic}(X)$ with $\deg(L) = m$, we have exactly $\frac{q^{m-g+1}-1}{q-1}$ effective divisors D with $\mathcal{O}_X(D) \simeq L$.

Let d_0 be the smallest nonnegative integer such that $d_0 e \geq 2g-1$. We deduce that

$$Z(X,t) = \sum_{D \geq 0, \deg(D) \leq 2g-2} t^{\deg(D)} + \sum_{d \geq d_0} h \frac{q^{de-g+1}-1}{q-1} t^{de}. \tag{2}$$

Note that the first sum in (2) is a polynomial in t^e of degree $\leq (2g-2)/e$. Since $\sum_{d \geq d_0} t^{de} = \frac{t^{d_0 e}}{1-t^e}$ and $\sum_{d \geq d_0} q^{de} t^{de} = \frac{(qt)^{d_0 e}}{1-(qt)^e}$, the second sum in (2) is equal to

$$\frac{h}{(q-1)} \cdot \left(q^{1-g} \cdot \frac{(qt)^{d_0 e}}{1-(qt)^e} - \frac{t^{d_0 e}}{1-t^e} \right). \tag{3}$$

We conclude that we may write

$$Z(X,t) = \frac{f(t^e)}{(1-t^e)(1-q^e t^e)}, \tag{4}$$

where f is a polynomial with rational coefficients of degree $\leq \max\{2 + \frac{2g-2}{e}, d_0 + 1\}$. In fact, since $Z(X,t)$ has integer coefficients, we see that f has integer coefficients, as well.

This already shows that $Z(X,t)$ is a rational function. We now show the more precise assertions in the statement of the theorem. Note first that the expression in (3) implies

that

$$\lim_{t\to 1}(t-1)Z(X,t) = -\frac{h}{q-1}\cdot\lim_{t\to 1}\frac{t-1}{1-t^e} = \frac{h}{e(q-1)}. \tag{5}$$

In particular, we see that $Z(X,t)$ has a pole of order one at $t=1$.

We now show that, in fact, $e=1$. Consider $X' = X\times_{\operatorname{Spec}\mathbf{F}_q}\operatorname{Spec}\mathbf{F}_{q^e}$. We have seen in Lecture 2, Proposition 3.8 that

$$Z(X',t^e) = \prod_{i=1}^{e} Z(X,\xi^i t),$$

where ξ is an e^{th} primitive root of 1. It follows from the formula in (4) that $Z(X',t^e) = Z(X,t)^e$. On the other hand, applying what we have proved so far to X', we see that $Z(X',t)$ has a pole of order one at $t=1$, and therefore $Z(X',t^e)$ has the same property. This implies that $e=1$. If $g\geq 0$, then $d_0 = 2g-1$, so that $\deg(f)\leq 2g$. On the other hand, $d_0 = 0$ if $g=0$, and the formula in (3) shows that $f=h$ in this case. The remaining assertions in the theorem now follow from (4) and (5). □

For future reference, we state explicitly the following result that was showed during the proof of Theorem 1.1.

Corollary 1.2. *If X is a smooth, geometrically connected, projective curve over $\mathbf{F}_q$, then all $\operatorname{Pic}^m(X)$ have the same (nonzero) number of elements.*

Remark 1.3. If X is a smooth, geometrically connected, projective curve of genus zero over $\mathbf{F}_q$, it follows from the previous corollary that there is a line bundle $L\in\operatorname{Pic}(X)$ with $\deg(L)=1$. This gives an isomorphism $X\simeq\mathbf{P}^1_{\mathbf{F}_q}$.

2. The functional equation

In our setting, if Δ is the diagonal in $\overline{X}\times\overline{X}$, then (Δ^2) can be computed via the adjunction formula: if $\ell_1 = \overline{X}\times\text{pt}$ and $\ell_2 = \text{pt}\times\overline{X}$, then $(\ell_1^2) = 0 = (\ell_2^0)$, $(\ell_1\cdot\ell_2) = 1$, and $(\Delta\cdot\ell_1) = 1 = (\Delta\cdot\ell_2)$. Therefore we have

$$2g-2 = (\Delta\cdot(\Delta + (2g-2)\ell_1 + (2g-2)\ell_2)) = (\Delta^2) + 2(2g-2).$$

Hence $(\Delta^2) = 2-2g$, and the statement of the second Weil conjecture for curves becomes the following.

Theorem 2.1. *If X is a smooth, geometrically connected, projective curve over $\mathbf{F}_q$, then*

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

Proof. As we will see, the key ingredient in the proof is Serre duality. If $g=0$, it follows from Remark 1.3 that $X\simeq\mathbf{P}^1_{\mathbf{F}_q}$. In this case $Z(X,t) = \frac{1}{(1-t)(1-qt)}$, and the formula in the theorem is straightforward to check (we did it for all projective spaces in Lecture 3). Hence from now on we may assume that $g\geq 1$. We follow the approach to $Z(X,t) = \sum_{D\geq 0} t^D$ used in the previous section.

Recall that for every line bundle $L \in \mathrm{Pic}(X)$ with $h^0(L) \geq 1$, the effective divisors D with $\mathcal{O}(D) \simeq L$ form the $\mathbf{F}_q$-points of a projective space $\mathbf{P}^{h^0(L)-1}$, hence there are $\frac{q^{h^0(L)}-1}{q-1}$ such divisors. Using the fact that $h^0(L) = \deg(L) - g + 1$ when $\deg(L) \geq 2g-1$ and Corollary 1.2, we conclude that

$$Z(X,t) = \sum_{m=0}^{2g-2} \left(\sum_{L \in \mathrm{Pic}^m(X)} \frac{q^{h^0(L)}-1}{q-1} \right) t^m + \sum_{m \geq 2g-1} h \frac{q^{d-g+1}-1}{q-1} t^d = S_1 + S_2, \tag{6}$$

where

$$S_1 = \sum_{m=0}^{2g-2} \sum_{L \in \mathrm{Pic}^m(X)} \frac{q^{h^0(L)}}{q-1} t^m, \; S_2 = -\frac{h}{q-1} \cdot \frac{1}{1-t} + \frac{hq^{1-g}(qt)^{2g-1}}{(q-1)(1-qt)}. \tag{7}$$

Note that

$$S_2(1/qt) = -\frac{h}{q-1} \cdot \frac{qt}{1-qt} - \frac{hq^{1-g}t^{2-2g}}{(q-1)(1-t)}$$

$$= q^{1-g}t^{2-2g} \cdot \left(\frac{hq^g t^{2g-1}}{(q-1)(1-qt)} - \frac{h}{(q-1)(1-t)} \right) = q^{1-g}t^{2-2g} S_2(t).$$

On the other hand, $L \to \omega_X \otimes L^{-1}$ gives a bijection between the set of line bundles on X of degree in $[0, 2g-2]$, and Serre duality plus Riemann-Roch gives $h^0(\omega_X \otimes L^{-1}) = h^0(L) - (\deg(L) - g + 1)$. Therefore

$$S_1(1/qt) = \sum_{m=0}^{2g-2} \left(\sum_{L \in \mathrm{Pic}^m(X)} \frac{q^{h^0(L)}}{q-1} \right) \left(\frac{1}{qt} \right)^m = \sum_{m=0}^{2g-2} \left(\sum_{L \in \mathrm{Pic}^m(X)} \frac{q^{h^0(\omega_X \otimes L^{-1})}}{q-1} \right) \left(\frac{1}{qt} \right)^{2g-2-m}$$

$$= \sum_{m=0}^{2g-2} \left(\sum_{L \in \mathrm{Pic}^m(X)} \frac{q^{h^0(L)-m+g-1}}{q-1} \right) (qt)^{m+2-2g} = t^{2-2g} q^{1-g} \sum_{m=0}^{2g-2} \left(\sum_{L \in \mathrm{Pic}^m(X)} \frac{q^{h^0(L)}}{q-1} \right) t^m$$

$$= q^{1-g}t^{2-2g} S_1(t).$$

This completes the proof of the theorem. □

Remark 2.2. With the notation in Theorem 1.1, we write $f(t) = \prod_{i=1}^{2g}(1 - \omega_i t)$, with $\omega_i \in \mathbf{C}$, possibly zero. We have

$$Z(X, 1/qt) = \frac{\prod_{i=1}^{2g} \left(1 - \frac{\omega_i}{qt}\right)}{\left(1 - \frac{1}{qt}\right)\left(1 - \frac{1}{t}\right)} = \frac{qt^2 (qt)^{-2g} \prod_{i=1}^{2g}(qt - \omega_i)}{(1-t)(1-qt)} = q^{1-g}t^{2-2g} \cdot \frac{\prod_{i=1}^{2g}(1 - \omega_i t)}{(1-t)(1-qt)},$$

where the last equality is a consequence of Theorem 2.1. Therefore $\prod_{i=1}^{2g}(t - \omega_i/q) = q^{-g} \cdot \prod_{i=1}^{2g}(1 - \omega_i t)$.

The first consequence is that $\omega_i \neq 0$ for all i, that is, $\deg(f) = 2g$. Furthermore, we see that $\prod_{i=1}^{2g} \omega_i = q^g$, and the multiset $\{\omega_1, \ldots, \omega_{2g}\}$ is invariants under the map $x \to q/x$.

Remark 2.3. Note that the assertion in the fourth Weil conjecture in now clear in our setting. Indeed, we have $B_0 = B_2 = 1$ and $B_1 = 2g$. Recall that $E = 2 - 2g$, hence $E = B_0 - B_1 + B_2$. Furthermore, if X is the closed fiber of a smooth projective curve $\widetilde{X}$ over a finite type $\mathbf{Z}$-algebra R, then $\widetilde{X}_{\mathbf{C}} := \widetilde{X} \times_{\operatorname{Spec} R} \operatorname{Spec} \mathbf{C}$ is a smooth connected complex curve of genus g. Its Betti numbers are $b_0 = b_2 = 1$, and $b_1 = 2g$ (the formula for b_1 is a consequence of Hodge decomposition: $b_1(\widetilde{X}_{\mathbf{C}}) = h^0(\Omega_{\widetilde{X}_{\mathbf{C}}}) + h^1(\mathcal{O}_{\widetilde{X}_{\mathbf{C}}}) = 2g$). This proves all the assertions in the fourth Weil conjecture for X.

3. The analogue of the Riemann hypothesis

We use the notation for the zeta function $Z(X,t)$ introduced in Remark 2.2:

$$Z(X,t) = \frac{\prod_{i=1}^{2g}(1-\omega_i t)}{(1-t)(1-qt)}. \tag{8}$$

The following proves the analogue of the Riemann hypothesis in our setting.

Theorem 3.1. *With the above notation, every ω_i is an algebraic integer, and $|\omega_i| = q^{1/2}$ for every i.*

Remark 3.2. If we show that $|\omega_i| \leq q^{1/2}$ for every i, since the multiset $\{\omega_1, \ldots, \omega_{2g}\}$ is invariant by the map $x \to q/x$ (see Remark 2.2) we conclude that we also have $|\omega_i| \geq q^{1/2}$, hence $|\omega_i| = q^{1/2}$ for every i. The fact that the ω_i are algebraic integers is clear: since $\prod_{i=1}^{2g}(1-\omega_i t) = (1-t)(1-qt)Z(X,t)$ has integer coefficients, it follows that all elementary symmetric functions $s_j = s_j(\omega_1, \ldots, \omega_{2g})$ are integers, and ω_i is a root of $t^{2g} + \sum_{j=1}^{2j}(-1)^j s_j t^{2g-j}$.

Before proving Theorem 3.1 we make some general considerations that are very useful in general when considering zeta functions of curves. Let $N_m = |X(\mathbf{F}_{q^m})|$, and let $a_m \in \mathbf{Z}$ be defined by

$$N_m = 1 - a_m + q^m. \tag{9}$$

It follows from the definition of the zeta function and from (8) that

$$\sum_{m\geq 1} \frac{N_m}{m} t^m = \sum_{i=1}^{2g} \log(1-\omega_i t) - \log(1-t) - \log(1-qt) = \sum_{m\geq 1} \frac{1}{m} \cdot \left(1 + q^m - \sum_{i=1}^{2g} \omega_i^m\right) t^m, \tag{10}$$

hence $a_m = \sum_{i=1}^{2g} \omega_i^m$ for every $m \geq 1$. The following lemma rephrases the condition in Theorem 3.1 as an estimate for the integers a_m. This estimate, in fact, is responsible for many of the applications of the Weil conjectures in the case of curves.

Lemma 3.3. *With the above notation, we have $|\omega_i| \leq g^{1/2}$ for every i if and only if $|a_m| \leq 2gq^{m/2}$ for every $m \geq 1$.*

Proof. One implication is trivial: since $a_m = \sum_{i=1}^{2g} \omega_i^m$, if $|\omega_i| \leq q^{1/2}$ for every i, it follows that $|a_m| \leq 2g^{m/2}$. For the converse, note that

$$\sum_{m\geq 1} a_m t^m = \sum_{i=1}^{2g} \sum_{m\geq 1} \omega_i^m t^m = \sum_{i=1}^{2g} \frac{\omega_i t}{1-\omega_i t}. \tag{11}$$

If $|a_m| \leq 2gq^{m/2}$ for all m, then for $t \in \mathbf{C}$ with $|t| < q^{-1/2}$ we have

$$|\sum_{m\geq 1} a_m t^m| \leq 2g \sum_{m\geq 1} (q^{1/2}|t|)^m = \frac{2gq^{1/2}|t|}{1-q^{1/2}|t|}. \tag{12}$$

Note that (11) implies that the rational function $\sum_{m\geq 1} a_m t^r$ has a pole at $t = 1/\omega_i$. The estimate in (12) implies that $1/|\omega_i| \geq q^{-1/2}$, as required. □

We can now prove the main result of this section.

Proof of Theorem 3.1. As it follows from Remark 3.2 and Lemma 3.3, it is enough to show that $|N_m - (q^m + 1)| \leq 2gq^{m/2}$ for every m. In fact, if we prove this for $m = 1$, then we may apply this to $X \times_{\operatorname{Spec} \mathbf{F}_q} \operatorname{Spec} \mathbf{F}_{q^m}$ in order to get the bound for $|N_m - (q^m + 1)|$.

We recall the description of N_1 given in Lecture 2, Proposition 2.4. Consider the smooth projective surface $S = \overline{X} \times \overline{X}$, where $\overline{X} = X \times_{\operatorname{Spec} \mathbf{F}_q} \operatorname{Spec} \overline{\mathbf{F}}_q$. We have two divisors on S, the diagonal Δ and the graph Γ of the morphism $\mathrm{Frob}_{\overline{X},q}$ on $\overline{X}$. The two divisors intersect transversely, and the number of intersection points is $(\Gamma \cdot \Delta) = |X(\mathbf{F}_q)|$.

It is an elementary consequence of the Hodge index theorem (see Proposition 3.4 below) that if $\ell_1 = \overline{X} \times \mathrm{pt}$ and $\ell_2 = \mathrm{pt} \times \overline{X}$, then for every divisor D on S we have

$$(D^2) \leq 2(D \cdot \ell_1) \cdot (D \cdot \ell_2). \tag{13}$$

Let us apply this for $D = a\Delta + b\Gamma$. Note that $(\Delta \cdot \ell_1) = (\Delta \cdot \ell_2) = 1$, while $(\Gamma \cdot \ell_1) = q$ and $(\Gamma \cdot \ell_2) = 1$.

We now compute (Γ^2) and (Δ^2) via the adjunction formula. Note that the canonical class K_S on S is numerically equivalent to $(2g-2)(\ell_1 + \ell_2)$. Since both Δ and Γ are smooth curves of genus g, we have

$$2g - 2 = (\Delta \cdot (\Delta + K_S)) = (\Delta^2) + 2(2g-2),$$

$$2g - 2 = (\Gamma \cdot (\Gamma + K_S)) = (\Gamma^2) + (q+1)(2g-2).$$

Therefore $(\Delta^2) = -(2g-2)$ and $(\Gamma^2) = -q(2g-2)$.

Applying (13) for $D = a\Delta + b\Gamma$ gives

$$-a^2(2g-2) - qb^2(2g-2) + 2abN_1 \leq 2(a+bq)(a+b).$$

After simplifying, we get

$$ga^2 - ab(q+1-N_1) + gqb^2 \geq 0.$$

Since this holds for all integer (or rational) a and b, it follows that $(q+1-N_1)^2 \leq 4qg^2$. Therefore $|N_1 - (q+1)| \leq 2gq^{1/2}$, as required. This completes the proof of Theorem 3.1. □

The following proposition is [Har, Exercise V.1.9].

Proposition 3.4. *Let C_1 and C_2 be smooth projective curves over an algebraically closed field, and let $S = C_1 \times C_2$. If $\ell_1 = C_1 \times \mathrm{pt}$ and $\ell_2 = \mathrm{pt} \times C_2$, then for every divisor D on S we have*

$$(D^2) \leq 2(D \cdot \ell_1)(D \cdot \ell_2).$$

Proof. Recall that the Hodge index theorem says that if E is a divisor on S such that $(E \cdot H) = 0$, where H is ample, then $(E^2) \leq 0$ (see [Har, Theorem 1.9]).

We apply this result for the ample divisor $H = \ell_1 + \ell_2$, and for $E = D - (b\ell_1 + a\ell_2)$, where $a = (D \cdot \ell_1)$ and $b = (D \cdot \ell_2)$. Note that $(E \cdot H) = 0$, hence $(E^2) \leq 0$. Since $(E^2) = (D^2) - 2ab$, we get the assertion in the proposition. □

Example 3.5. Consider the case when X is an elliptic curve (that is, $g = 1$). In this case it follows from Theorem 3.1 and Remark 2.2 that

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

where $|\alpha| = |\beta| = q^{1/2}$, and $a \in \mathbf{Z}$. Note that $|X(\mathbf{F}_{q^m})| = (1+q^m) - 2\mathrm{Re}(\alpha^m)$. In particular, $a = (1+q) - |X(\mathbf{F}_q)|$.

References

[Lor] D. Lorenzini, *An invitation to arithmetic geometry*, Graduate studies in Mathematics 9, American Mathematical Society, Providence, RI, 1996. 2

[Har] R. Hartshorne, *Algebraic Geometry*, Graduate Texts in Mathematics, No. 52, Springer-Verlag, New York-Heidelberg, 1977. 1, 7