THE WEIL CONJECTURES FOR CURVES

SAM RASKIN

Abstract. This paper is a report for the 2007 University of Chicago REU. It is based on a series of lectures given by Sasha Beilinson in the spring of 2007. We give an introduction to the Weil conjectures for varieties over finite fields and prove them for curves using basic techniques of algebraic geometry. The author would like to express his gratitude to his friend and mentor Mitya Boyarchenko for the crucial guidance he provided this summer.

Contents

1. Zeta functions and Weil conjectures

1.1. **Introduction.** We begin with an overview of the properties of general zeta functions. Let X be a scheme of finite type over $\mathbb{Z}$ throughout this section and let $|X|$ denote the set of closed points of X. If $x \in |X|$, we write $\Bbbk_x$ for the residue field of X at x. Note that $\Bbbk_x$ is finite because of the following version of the Nullstellensatz "over $\mathbb{Z}$":

Lemma 1.1. *If A is a field which is finitely generated as a ring, then A is finite.*

Proof. We thank Akaki Tikaradze for showing us the following slick argument. If A has characteristic $p > 0$, then A is finitely generated as an algebra over $\mathbb{F}_p$ and we can apply the usual Nullstellensatz. Otherwise the natural homomorphism $\mathbb{Z} \longrightarrow A$ is injective, so A is torsion-free, and hence flat, as a $\mathbb{Z}$-module. Moreover, the natural morphism $\mathrm{Spec}(A) \longrightarrow \mathrm{Spec}(\mathbb{Z})$ is of finite type; being flat, it is therefore open. But this is a contradiction: since A is a field of characteristic zero, the image of this morphism must consist only of the generic point of $\mathrm{Spec}(\mathbb{Z})$. □

Because of this fact, we can make the following definition:

Definition 1.2. The **zeta function** of X is the formal product:

$$\zeta(X,s) = \prod_{x\in|X|} (1-|\Bbbk_x|^{-s})^{-1}$$

Here, s is a complex variable, and each factor $(1-|\Bbbk_x|^{-s})^{-1}$ in the product above is viewed as a meromorphic function of s. *A priori*, it is not clear how to make sense out of this formal product. There are two approaches to this. On one hand, the product is known to converge when the real part of s is large enough (cf. Proposition 1.6 below). On the other hand, if X is a scheme of finite type over a finite field $\mathbb{F}_q$, then a change of variables $t = q^{-s}$ transforms $\zeta(X,s)$ into a formal power series in the variable t.

Examples 1.3. (1) If $X = \mathrm{Spec}(\mathbb{Z})$, then $\zeta(X,s)$ is just the classical Riemann zeta function. More generally, if $\mathcal{O}$ is the ring of integers of a number field K, then $\zeta(\mathrm{Spec}(\mathcal{O}),s)$ is the Dedekind zeta function of K.

(2) If X is a scheme of finite type over $\mathbb{F}_q$, then one usually makes the change of variables $t = q^{-s}$ and defines:

$$\zeta(X,s) = Z(X,q^{-s}) = Z(X,t) = \prod_{x\in|X|} (1-t^{\deg(x)})^{-1}$$

Here, if $|\Bbbk_x| = q^n$, we define $\deg(x) = n$. By Lemma 1.4, the infinite product on the right hand side gives a well defined formal power series in the variable t with rational coefficients. This is a useful change of variables in view of Proposition 1.5, which shows that the zeta function of X is closely related to the generating function for the numbers $|X(\mathbb{F}_{q^n})|$ of points of X over finite extensions of $\mathbb{F}_q$. This result was in fact the original motivation for introducing the zeta functions of algebraic varieties over finite fields (cf. [We49]).

Lemma 1.4. *If X is a scheme of finite type over $\mathbb{F}_q$, then $\big|X(\mathbb{F}_{q^n})\big| = O\big(q^{n\cdot\dim X}\big)$ as $n\to\infty$. A fortiori, for any $N\in\mathbb{N}$, the number of $x\in|X|$ with $\deg(x)\leq N$ is finite.*

Proof. It is clear that we may assume that X is reduced and irreducible (cf. the proof of Proposition 1.6 below). In this case, by Noether's normalization lemma, there is a finite morphism $U \xrightarrow{\varphi} \mathbb{A}^{\dim(X)}_{\mathbb{F}_q}$ for $U\subset X$ a dense open subset. Hence:

$$|U(\mathbb{F}_{q^n})| \leq \deg(\varphi)\cdot q^{n\cdot\dim(X)}$$

Because $\dim(X\setminus U) < \dim(X)$, we have the result by induction on $\dim(X)$. □

Proposition 1.5. *We have* $t\cdot\dfrac{d}{dt}\log Z(X,t) = \displaystyle\sum_{n\geq 1} |X(\mathbb{F}_{q^n})|\cdot t^n$ *in* $\mathbb{Q}[[t]]$.

Proof. We formally compute:

$$\begin{aligned} t \cdot \frac{d}{dt} \log\ Z(X,t) &= t \cdot \sum_{x \in |X|} \frac{d}{dt} \log((1-t^{\deg(x)})^{-1}) \\ &= \sum_{x \in |X|} \deg(x) \cdot \frac{t^{\deg(x)}}{1-t^{\deg(x)}} \\ &= \sum_{x \in |X|} \deg(x) \cdot \sum_{k \geq 1} t^{k \cdot \deg(x)} \\ &= \sum_{x \in |X|} \sum_{\deg(x) | n} \deg(x) t^n \end{aligned}$$

Because $|X(\mathbb{F}_{q^n})|$ is exactly the number of closed points of X of degree dividing n, with each such point x counted $\deg(x)$ many times, this last sum is $\sum_{n \geq 1} |X(\mathbb{F}_{q^n})| \cdot t^n$. □

1.2. **The zeta function as an analytic function.** Since we are mainly interested in the zeta functions of varieties over finite fields, we will only give a full proof of the next result in this special case.

Proposition 1.6. *On compact subsets of* $U = \left\{ s \in \mathbb{C} \,\middle|\, \mathrm{Re}(s) > \dim(X) \right\}$*, the product defining* $\zeta(X,s)$ *converges absolutely and uniformly, and hence defines an analytic function on* U *(which justifies the terminology "zeta function").*

Proof. We reduce first to the case where X is integral (this part of the proof works in general). For, with X_{red} the reduced scheme associated to X, one clearly has:

$$\zeta(X,s) = \zeta(X_{red},s).$$

Therefore, we may assume X is reduced. Furthermore, if $X = X_1 \cup X_2$ for X_i closed subschemes of X, then with $X_1 \cap X_2$ the set theoretic intersection of X_1 and X_2 with the inherited reduced subscheme structure:

$$\zeta(X,s) = \frac{\zeta(X_1,s) \cdot \zeta(X_2,s)}{\zeta(X_1 \cap X_2, s)}$$

Thus, we may assume that X is irreducible as well. Because X is now assumed to be reduced and irreducible, it is integral.

Observe that now there are only two possibilities:

(1) X lies over a single closed point of $\mathrm{Spec}(\mathbb{Z})$, or else
(2) X is "spread over $\mathbb{Z}$," that is, the morphism $X \longrightarrow \mathrm{Spec}(\mathbb{Z})$ is dominant.

Indeed, if $X \longrightarrow \mathrm{Spec}(\mathbb{Z})$ is not dominant, its image is not dense and hence finite; thus it must consist of only one closed point of $\mathrm{Spec}(\mathbb{Z})$ as X is irreducible.

As mentioned before, we will only prove the result for case (1). Suppose that X lies above a single closed point p of $\mathrm{Spec}(\mathbb{Z})$, that is, that X is a scheme over $\mathbb{F}_p$ of finite type. To prove the convergence of $\zeta(X,s)$ for $\mathrm{Re}(s) > \dim(X)$, it suffices to prove the convergence of the power series $t \cdot \frac{d}{dt} \log Z(X,t)$ for $0 < t < q^{\dim(X)}$. This is clear because:

$$t \cdot \frac{d}{dt} \log Z(X,t) = \sum_{n \geq 1} |X(\mathbb{F}_{p^n})| t^n \leq M \cdot \sum_{n \geq 1} q^{n \cdot \dim(X)} t^n = M \cdot \sum_{n \geq 1} (q^{\dim(X)} t)^n,$$

where we have used the estimate of Lemma 1.4. □

1.3. **The Weil conjectures.** In a celebrated paper [We49], A. Weil stated three conjectures describing the properties of the power series $Z(X,t)$ for smooth projective varieties X over $\mathbb{F}_q$. He proved these conjectures in case $\dim X = 1$ earlier [We48]. The first two conjectures were proved in full generality by M. Artin and A. Grothendieck in the early 1960s (see [Gr64] and SGA 5); an independent proof (using completely different techniques) of the first one was also found by B. Dwork [Dw60]. The third conjecture was proved by P. Deligne about ten years later [De74].

We state these conjectures following Weil [We49] rather closely. *We assume that X is a projective scheme over $\mathbb{F}_q$ such that $X \times_{\mathrm{Spec}(\mathbb{F}_q)} \mathrm{Spec}(\overline{\mathbb{F}_q})$ is irreducible and nonsingular.*

1.3.1. *Rationality.* $Z(X,t)$ is the power series expansion of a rational function of t.

Assuming this conjecture, we will, by a slight abuse of notation, write $Z(X,t)$ both for the formal power series introduced before and for the corresponding rational function.

1.3.2. *Functional equation.* The function $Z(X,t)$ satisfies an identity of the form

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

where $d = \dim X$ and e is the Euler characteristic of X.

We note that, in general, the Euler characteristic of X can be defined as the self-intersection number of the diagonal in the product $X \times X$. However, we do not have to go into the details of this definition, since in the rest of the paper we only consider the case where X is a curve, and then the Euler characteristic of X can be defined in an *ad hoc* manner motivated by classical topology: $e = 2 - 2g$, where g is the genus of X.

1.3.3. *Riemann hypothesis.* Letting $d = \dim X$ as before, it is possible to write

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

where the $P_j(t)$ are polynomials with integer coefficients such that $P_0(t) = 1 - t$, $P_{2d}(t) = 1 - q^d t$, and, for $1 \leq j \leq 2d-1$, one has $P_j(t) = \prod_{i=1}^{b_j} (1 - \alpha_{ij} t)$, where $|\alpha_{ij}| = q^{j/2}$.

1.4. **Meromorphic continuation.** We conclude this section with a remark which will not be used anywhere in the text, but is interesting in its own right. Let us return to the more general setup considered at the beginning of this section: namely, let X be any scheme of finite type over $\mathrm{Spec}(\mathbb{Z})$. In view of Proposition 1.6, the formal product $\zeta(X,s)$ defines an analytic function in the half-plane $\left\{s \in \mathbb{C} \,\middle|\, \mathrm{Re}(s) > \dim(X)\right\}$, and it is natural to ask whether $\zeta(X,s)$ can be meromorphically continued to the whole complex plane. In the case where X is a smooth projective scheme over $\mathbb{F}_q$, the answer is positive in view of the first Weil conjecture (stated in §1.3), which implies that, in fact, $\zeta(X,s) = Z(X,q^{-s})$ for a rational function $Z(X,t)$.

More generally, if the canonical morphism $X \longrightarrow \mathrm{Spec}(\mathbb{Z})$ is *not* dominant, one can easily prove, using the ℓ-adic cohomology techniques developed in SGA 5, that $\zeta(X,s)$ is a product of functions of the form $Z_p(p^{-s})$, where each $Z_p(t)$ is a rational function and p runs through the finitely many primes such that $p\mathbb{Z}$ is in the image of $X \longrightarrow \mathrm{Spec}(\mathbb{Z})$.

On the other hand, for the Dedekind zeta-function $\zeta_K(s)$ of a number field K, meromorphic continuation is a very classical result (of course, $\zeta_K(s)$ is very far from being expressible in terms of rational and exponential functions).

However, if, say, X is integral, the canonical morphism $X \longrightarrow \mathrm{Spec}(\mathbb{Z})$ *is* dominant, and $\dim X > 1$, the question of whether $\zeta(X,s)$ admits meromorphic continuation to all of $\mathbb{C}$ still remains open. The best result known to us is that $\zeta(X,s)$ can be analytically continued to the half-plane $\left\{s \in \mathbb{C} \,\middle|\, \mathrm{Re}(s) > \dim(X) - \frac{1}{2}\right\}$.

1.5. **Structure of the text.** In this paper we present proofs of the Weil conjectures for smooth projective curves over finite fields. We will begin in §2 by proving the rationality and functional equation using the Riemann-Roch theorem and Serre duality for curves. The remainder of the paper will be centered around the proof of the Riemann hypothesis. The main technique used will be intersection theory on surfaces, reviewed in §5.

2. Rationality and the functional equation

2.1. **Setup of this section.** Throughout this section we fix a field $\Bbbk$ and a smooth projective geometrically connected curve X_0 over $\Bbbk$. Starting with §2.4, we will take $\Bbbk$ to be finite. The reader will notice that many of the definitions and results recalled in this section remain valid after relaxing some of our assumptions, but for consistency, we decided to work within a single framework.

Recall that to say that X_0 is geometrically connected means that

$$X = X_0 \times_{\mathrm{Spec}(\Bbbk)} \mathrm{Spec}(\overline{\Bbbk})$$

is connected. The choice of the notation X_0 and X is rather standard in the study of varieties over finite fields (see, e.g., [De74] or SGA4$\frac{1}{2}$).

2.2. **Line bundles and divisors.** In order to prove the rationality of the zeta function of a smooth curve over $\mathbb{F}_q$, we will need a few elementary ideas and facts about line bundles on curves. Recall that the **Picard group** of X_0 is the set $\mathrm{Pic}(X_0)$ of isomorphism classes of line bundles of X_0 given a group structure through the tensor product. We write $\mathrm{Div}(X_0)$ for the group of Weil divisors on X_0 (i.e., formal finite linear combinations of closed points of the underlying scheme of X_0 with integral coefficients).

If $D \in \mathrm{Div}(X_0)$, we denote the degree of D by $\deg(D) \in \mathbb{Z}$. Let us recall its definition. If $D = \sum_{x \in |X_0|} n_x \cdot x$, where $|X_0|$ is the set of closed points of X_0 and $n_x \in \mathbb{Z}$, then $\deg(D) = \sum n_x \cdot \deg(x)$, where $\deg(x) = [\Bbbk_x : \Bbbk]$ and $\Bbbk_x$ denotes the residue field of X_0 at x (the extension $\Bbbk \subset \Bbbk_x$ is finite in view of the Nullstellensatz).

Remark 2.1. Because X_0 is smooth, there is a canonical isomorphism between the groups of Weil and Cartier divisors on X_0. Furthermore, one has a natural bijection between the set of effective Cartier divisors on X_0 and the set of line bundles on X_0 equipped with a non-zero global section modulo scaling. For details on these two bijections, see [Mu66], §9. Under these correspondences, isomorphism of line bundles translates to linear equivalence of divisors, so $\mathrm{Pic}(X_0)$ is isomorphic to $\mathrm{Div}(X_0)/\{\text{divisors linearly equivalent to } 0\}$.

Let us write $\mathcal{K}(X_0)$ for the field of rational functions on X_0. Since X_0 is projective, if $f \in \mathcal{K}(X_0)^*$ and (f) denotes the divisor defined by f, then $\deg((f)) = 0$. Thus, the degree homomorphism $\mathrm{Div}(X_0) \longrightarrow \mathbb{Z}$ descends to give a homomorphism $\mathrm{Pic}(X_0) \longrightarrow \mathbb{Z}$.

Definition 2.2. We set $\mathrm{Pic}^0(X_0)$ to be the kernel of the latter homomorphism.

2.3. **The Riemann-Roch theorem.** We keep the assumption of §2.1.

Recall the following theorem of Riemann-Roch-Serre which is crucial in discussing line bundles on projective curves. If $\mathscr{L}$ is a line bundle on X_0, we denote by $h^i(\mathscr{L})$ the $\Bbbk$-dimension of $H^i(X_0, \mathscr{L})$. Of course, as we only need the zero-th cohomology in this formulation, the reader uncomfortable with sheaf cohomology may rest assured that $H^0(X_0, \mathscr{L}) = \Gamma(X_0, \mathscr{L})$. We denote by ω_{X_0} the sheaf of differential 1-forms on X_0.

Theorem 2.3 (Riemann-Roch formula)**.** *For $\mathscr{L}$ a line bundle on X_0, we have*

$$h^0(\mathscr{L}) - h^0(\omega_{X_0} \otimes \mathscr{L}^{-1}) = \deg(\mathscr{L}) + 1 - g,$$

where $g = h^0(\omega_{X_0})$ is the genus of X_0.

For the proof, see, for instance, §VIII.1 of [AK70].

Corollary 2.4. *If $\deg(\mathscr{L}) > 2g - 2$, then $h^0(\mathscr{L}) = \deg(\mathscr{L}) + 1 - g$.*

Proof. Suppose first that D is a Weil divisor on X_0 corresponding to a line bundle $\mathcal{E}$. Recall that if $f \in \mathcal{K}(X_0)^*$, then $\deg(f) = 0$ because X_0 is projective. Thus if $0 \neq f \in \Gamma(X_0, \mathcal{E})$, then by definition $(f) + D \geq 0$, and therefore $\deg(D) = \deg((f) + D)) \geq 0$.

Because $\deg(\omega_{X_0}) = 2g-2$, as one easily checks using the Riemann-Roch formula, setting $\mathcal{E} = \omega_{X_0} \otimes \mathscr{L}^{-1}$ we have $\deg(\mathcal{E}) < 0$ which implies that $\mathcal{E}$ has no global sections, that is, $h^0(\omega_{X_0} \otimes \mathscr{L}^{-1}) = 0$. The result now follows immediately from the Riemann-Roch formula. □

We need one last result before proving the rationality of $Z(X_0, t)$:

Proposition 2.5. *With the assumption of §2.1, the subgroup* $\mathrm{Pic}^0(X_0) \subset \mathrm{Pic}(X_0)$ *has a coset all of whose elements admit representatives by effective divisors in* $\mathrm{Div}(X_0)$. *In particular, if* $\Bbbk$ *is finite, then* $\mathrm{Pic}^0(X_0)$ *is finite.*

Proof. Let $n > 2g$ and consider any divisor D of degree n. By Corollary 2.4, $h^0(\mathcal{O}(D)) = \deg(D) + 1 - g = n + 1 - g > 0$. However, as noted in the proof of the corollary, if $h^0(\mathcal{O}(D)) > 0$, then D must be linearly equivalent to an effective divisor. Clearly, the set of all divisors of degree n on X_0 modulo linear equivalence is a coset of $\mathrm{Pic}^0(X_0)$.

The second statement of the proposition follows because if $\Bbbk$ is finite, then for a fixed $n \in \mathbb{N}$, the number of closed points of X_0 of degree at most n is finite (Lemma 1.4). □

2.4. **Rationality.** We keep the assumptions of §2.1 and put $\Bbbk = \mathbb{F}_q$.

Theorem 2.6. *With the hypotheses above,* $Z(X_0, t)$ *is a rational function of* t.

Proof. Computing formally with the product in the definition of Z, we see that:

$$Z(X_0, t) := \prod_{x \in |X_0|} \left(1 - t^{\deg(x)}\right)^{-1} = \prod_{x \in |X_0|} \sum_{k=0}^{\infty} t^{k \cdot \deg(x)}.$$

Expanding the product on the right, we see that it is the sum over all possible terms $t^{\sum k_i \deg(x_i)}$ where the sum in the exponent is finite and the k_i are positive integers. That is, the sum is equal to $\displaystyle\sum_{D \geq 0} t^{\deg(D)}$ where the sum is taken over effective divisors on X_0. Now, to each such divisor we may assign a pair $(\mathscr{L}, \gamma)$, where γ is a global section of $\mathscr{L}$. As the divisors correspond to such a pair up to a scalar multiple of γ, we see that our sum has evolved into the expression:

$$\sum_{\mathscr{L} \in \mathrm{Pic}(X_0), \mathscr{L} \geq 0} |\mathbb{P}(\Gamma(X_0, \mathscr{L}))| \cdot t^{\deg(\mathscr{L})} = \sum_{\mathscr{L} \in \mathrm{Pic}(X_0), \mathscr{L} \geq 0} \frac{q^{h^0(\mathscr{L})} - 1}{q - 1} \cdot t^{\deg(\mathscr{L})}.$$

With the sum in this form, we may apply the Riemann-Roch theorem and Corollary 2.4 to compute:

$$\sum_{0 \leq \deg(\mathscr{L}) \leq 2g-2} \frac{q^{h^0(\mathscr{L})} - 1}{q - 1} \cdot t^{\deg(\mathscr{L})} + \sum_{2g-2 < \deg(\mathscr{L})} \frac{q^{h^0(\mathscr{L})} - 1}{q - 1} \cdot t^{\deg(\mathscr{L})} =$$

$$\sum_{0 \leq \deg(\mathscr{L}) \leq 2g-2} \frac{q^{h^0(\mathscr{L})} - 1}{q - 1} \cdot t^{\deg(\mathscr{L})} + \sum_{2g-2 < \deg(\mathscr{L})} \frac{q^{\deg(\mathscr{L})+1-g} - 1}{q - 1} \cdot t^{\deg(\mathscr{L})}.$$

Let us define

$$g_1(t) = \sum_{0 \leq \deg(\mathscr{L}) \leq 2g-2} \frac{q^{h^0(\mathscr{L})} - 1}{q-1} \cdot t^{\deg(\mathscr{L})}$$

and

$$g_2(t) = \sum_{2g-2 < \deg(\mathscr{L})} \frac{q^{\deg(\mathscr{L})+1-g} - 1}{q-1} \cdot t^{\deg(\mathscr{L})}.$$

By Proposition 2.5, the group $\mathrm{Pic}^0(X_0)$ is finite. Thus, because there are $|\mathrm{Pic}^0(X_0)|$ line bundles on X_0 of degree n, $g_1(t)$ is a polynomial of degree $2g-2$ and we see that:

$$g_2(t) = |\mathrm{Pic}^0(X_0)| \sum_{2g-2 < n} \frac{q^{n+1-g} - 1}{q-1} \cdot t^n = \frac{h(t)}{(1-t)(1-qt)}.$$

The equality is of course justified by the formula for the summation of a geometric series, which shows as well that the degree of $h(t)$ is $2g$. □

The proof given above yields a stronger version of Theorem 2.6:

Theorem 2.7. *We have*

$$Z(X_0, t) = \frac{f(t)}{(1-t)(1-qt)},$$

where $f(t) \in \mathbb{Q}[t]$ has degree at most $2g$ and constant term 1.

2.5. **The functional equation.** Here our setup is as in §2.4. We will prove the functional equation for the zeta function (i.e., the second Weil conjecture) for X_0 by considering the proof of Theorem 2.6 in greater detail.

Theorem 2.8. $Z(X_0, q^{-1}t^{-1}) = q^{1-g}t^{2-2g}Z(X_0, t)$.

To motivate the proof of this result, we first make the following observation.

Computation 2.9. We consider for a moment, using the notation of the proof of Theorem 2.6, the polynomial

$$g_1(t) = \sum_{0 \leq \deg(\mathscr{L}) \leq 2g-2} \frac{q^{h^0(\mathscr{L})} - 1}{q-1} \cdot t^{\deg(\mathscr{L})}.$$

We can involute these line bundles by sending $\mathscr{L}$ to $\omega_{X_0} \otimes \mathscr{L}^{-1}$, recalling again that $\deg(\omega_X) = 2g-2$. Let us observe what Serre duality tells us happens to a typical summand of g_1 upon applying this involution:

$$\begin{aligned}
\frac{q^{h^0(\omega_{X_0} \otimes \mathscr{L}^{-1})} - 1}{q-1} \cdot t^{\deg(\omega_{X_0} \otimes \mathscr{L}^{-1})} &= \frac{q^{h^0(\mathscr{L}) - \deg(\mathscr{L}) - 1 + g} - 1}{q-1} \cdot t^{2g-2-\deg(\mathscr{L})} \\
&= \frac{q^{h^0(\mathscr{L})} - q^{\deg \mathscr{L} + 1 - g}}{q-1} \cdot q^{\deg(\mathscr{L})+1-g} t^{2g-2-\deg(\mathscr{L})} \\
&= q^{g-1}t^{2g-2} \cdot \frac{q^{h^0(\mathscr{L})} - q^{\deg(\mathscr{L})+1-g}}{1-g} \cdot (q^{-1}t^{-1})^{\deg(\mathscr{L})}
\end{aligned}$$

While the last expression may seem at first foreboding, we note that

$$\frac{q^{h^0(\mathscr{L})}-1}{q-1} = \frac{q^{h^0(\mathscr{L})}-q^{\deg(\mathscr{L})+1-g}}{q-1} + \frac{q^{\deg(\mathscr{L})+1-g}-1}{q-1}$$

and reassuringly observe that the right summand resembles the typical summand of g_2. With this encouragement, we feel prepared to approach the functional equation for Z.

Proof. Using Computation 2.9 and the symmetry of $\mathscr{L} \mapsto \omega_{X_0} \otimes \mathscr{L}^{-1}$, we see that the expression

$$\sum_{0\le\deg(\mathscr{L})\le g-1} \frac{q^{h^0(\mathscr{L})}-1}{q-1} t^{\deg \mathscr{L}} + \sum_{g\le\deg\mathscr{L}\le 2g-2} \frac{q^{h^0(\mathscr{L})}-q^{\deg(\mathscr{L})+1-g}}{q-1} t^{\deg(\mathscr{L})}$$

satisfies the functional equation. As noted at the end of the computation, we have $Z(X_0,t)$ is the sum of this expression and

$$\begin{aligned}\sum_{\deg(\mathscr{L})\ge g} \frac{q^{\deg(\mathscr{L})+1-g}-1}{q-1} t^{\deg(\mathscr{L})} &= |\operatorname{Pic}^0(X_0)| \sum_{n\ge g} \frac{q^{n+1-g}-1}{q-1} t^n \\ &= |\operatorname{Pic}^0(X_0)| t^g (1-t)^{-1}(1-qt)^{-1}.\end{aligned}$$

However, it is trivial to check that this last expression satisfies the functional equation, so we have completed the proof. □

The following is an equivalent reformulation of the functional equation:

Corollary 2.10. (*a*) *With notation as in Theorem 2.7, $f(t)$ has degree exactly $2g$.*
(*b*) *We may write $f(t) = \prod_{i=1}^{2g}(1-\omega_i t)$, where $\omega_i \in \mathbb{C}$ are ordered in such a way that $\omega_i \omega_{2g+1-i} = q$ for all i.*

Proof. By Theorem 2.8:

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

This immediately gives $t^{2g}q^g f(q^{-1}t^{-1}) = f(t)$. Comparing degrees, we get $2g = \deg(f)$. Furthermore, these polynomials must have the same sets of roots. The left expression has roots $\left\{\frac{\omega_i}{q}\right\}_{i=1}^{2g}$, so there must be some permutation $\sigma \in S_{2g}$ such that $\omega_i\omega_{\sigma(i)} = q$. Because f has rational (and hence real) coefficients, it has an even number of real roots which means $\sqrt{q}$ and $-\sqrt{q}$ appear as roots both an even number of times or both an odd number of times. Also, the leading coefficient of f equals q^g, so since f has constant term 1, the product of its roots must be positive. Thus, both appear an even number of times. This allows us the precise formulation about the ordering as given above. □

3. The Riemann hypothesis for curves

3.1. **Statement of the result.** In this section we remain in the setup of §2.4. Thus X_0 is a smooth projective geometrically connected curve over $\mathbb{F}_q$ and $X = X_0 \otimes_{\mathbb{F}_q} \overline{\mathbb{F}}_q$. We will state more explicitly the third of the Weil conjectures (see §1.3) for X_0 and discuss an equivalent reformulation thereof.

Because the zeta function $Z(X_0, t)$ has rational coefficients, its zeroes appear in complex conjugate pairs. It then becomes a natural question to ask whether the pairing given by Corollary 2.10 is the same as this conjugate pairing, that is, if:

$$\frac{q}{\omega_i} = \overline{\omega_i}$$

The answer is positive:

Theorem 3.1. *In the notation of Corollary 2.10, $|\omega_i| = q^{1/2}$ for all i.*

We prove this result in Section 6. It is called the Riemann hypothesis for curves over finite fields because of the analogy with the classical case, for, after our change of variables from Example 1.3(2), this is exactly the claim that every zero of $\zeta(X_0, s)$ has real part $\frac{1}{2}$.

3.2. **A reformulation.** The proof of the Riemann hypothesis for curves that we give in Section 6 is based on the following fact.

Proposition 3.2. *The Riemann hypothesis holds for X_0 if and only if*

$$|X_0(\mathbb{F}_{q^n})| = q^n + O(q^{n/2}) \quad \text{as } n \to \infty.$$

Proof. Suppose first that $|\omega_i| = q^{1/2}$ for all i. Consider the equality:

$$\frac{\prod_{i=1}^{2g}(1 - \omega_i t)}{(1-t)(1-qt)} = Z(X_0, t)$$

Taking logarithmic derivatives of both sides and multiplying by t yields:

$$\sum_{n \geq 1}(1 + q^n - \sum_{i=1}^{2g} \omega_i^n)t^n = \sum_{n \geq 1} |X_0(\mathbb{F}_{q^n})| t^n.$$

Thus, $|X_0(\mathbb{F}_{q^n})| = 1 + q^n - \sum_{i=1}^{2g} \omega_i^n = q^n + O(q^{n/2})$ as $n \to \infty$.

Conversely, suppose that this estimate holds. The argument above shows that $\sum_{i=1}^{2g} \omega_i^n = O(q^{\frac{n}{2}})$. We use the following elementary lemma:

Lemma 3.3. *If $\lambda_1, ..., \lambda_k$ are complex numbers such that $|\sum_{i=1}^{k} \lambda_i^n|$ is bounded as a function of n, then $|\lambda_i| \leq 1$ for all i.*

Proof. We give a sketch of the proof because the details would be distracting and because this can be proved by an advanced high school student. Using the pigeonhole principle, there exist arbitrarily large N such that $\mathrm{Re}(\lambda_i^N) > 0$ and $-\frac{\mathrm{Re}(\lambda_i^N)}{2} < \mathrm{Im}(\lambda_i^N) < \frac{\mathrm{Re}(\lambda_i^N)}{2}$ for all i. However, this implies by an induction argument on k that:

$$\sqrt{2}^k \left| \sum_{i=1}^{k} \lambda_i^N \right| \geq \sum_{i=1}^{k} |\lambda_i|^N$$

Because the left hand side is bounded by assumption, the right hand side must be too. However, this is the case only if $|\lambda_i| \leq 1$ for all i. □

Applying this lemma to $\lambda_i = \omega_i q^{-\frac{n}{2}}$, we see that $|\omega_i| \leq q^{\frac{n}{2}}$ for all i. Together with Corollary 2.10, this yields:

$$|\omega_i| = \frac{q}{|\omega_{2g+1-i}|} \geq q^{\frac{n}{2}}$$

Thus, $|\omega_i| = q^{\frac{1}{2}}$ for all i. □

3.3. **Remarks.**

(1) One should think of Proposition 3.2 as something of an analogy to the statement that the classical Riemann hypothesis is equivalent to the estimate:

$$\pi(x) = \int_2^x \frac{dx}{\log(x)} + O(\sqrt{x}\log(x))$$

The reason for this is that computing $|X(\mathbb{F}_{q^n})|$ is like counting the number of maximal ideals in a ring of degree less than n.

(2) It is possible to give a more elementary proof of the Riemann hypothesis for curves (which is also based on Proposition 3.2) than the one we present in Section 6. This more elementary proof uses only the Riemann-Roch theorem on X itself, as opposed to the Riemann-Roch theorem on $X \times X$ (as in Weil's original argument), or intersection theory on $X \times X$ (as in Section 6 below).

The idea of a more elementary proof is due to S.A. Stepanov [St69], who proved the Riemann hypothesis for curves in some special cases. His method was further developed by E. Bombieri, who gave a complete proof in [Bo74]. However, this method is much less conceptual than the one due to Weil, so we do not discuss it.

4. Operations on divisors

In the next two sections, we will develop pull backs and push forwards on divisors and then the basics of intersection theory. These will then be applied to the Riemann hypothesis in concluding final section. A discussion of why these are the natural techniques to use will be given in the beginning of Section 5, where it is more appropriately located.

4.1. **Pull backs.** Consider a finite surjective morphism $\varphi : Y \longrightarrow Z$ between two normal integral schemes of finite type over a field $\Bbbk$. We will eventually associate to it two operations, the pull back $\varphi^* : \mathrm{Div}(Z) \longrightarrow \mathrm{Div}(Y)$ and the push forward $\varphi_* : \mathrm{Div}(Y) \longrightarrow \mathrm{Div}(Z)$, where $\mathrm{Div}(Y)$ denotes the group of Weil divisors on Y.

Definition 4.1. Let $y \in Y$ be a codimension 1 point[1] such that $\varphi(y) = z$ has codimension 1 in Z. This gives us an inclusion of the discrete valuation rings[2] $\mathcal{O}_{Z,z} \hookrightarrow \mathcal{O}_{Y,y}$. For t a uniformizer of $\mathcal{O}_{Y,y}$, we define the **ramification index** at y to be $e(y) = v_z(t)$, where $v_z : \mathcal{O}_{Z,z} \setminus \{0\} \longrightarrow \mathbb{Z}$ is the natural valuation. We set the convention that if $\varphi(y)$ has codimension at least 2, then $e(y) = 0$.

For y a point of codimension 1, we denote by $[y] = \overline{\{y\}}$ the corresponding prime divisor.

Definition 4.2. For $z \in Z$ a point of codimension 1, define the **pull back** of $[z]$ along φ by $\varphi^*([z]) = \sum_{\varphi(y)=z} e(y)[y]$. Extend this by linearity to give the definition of the pull back of an arbitrary divisor.

Lemma 4.3. *Pull backs take principal divisors to principal divisors and therefore define a map* $\mathrm{Pic}(Z) \longrightarrow \mathrm{Pic}(Y)$.

Proof. Let $f \in \mathcal{K}(Z)^*$. Consider the image $\tilde{f}$ of f under the inclusion $\mathcal{K}(Z) \xrightarrow{i} \mathcal{K}(Y)$ induced by φ. We claim that $(\tilde{f}) = \varphi^*((f))$. Evidently this statement is true if and only if it is true locally. (Here, "local" means local both on Y and on Z; we are implicitly using the fact that pullbacks are defined for any, not necessarily finite, morphism.) Therefore, we may reduce to the case where $Y = \mathrm{Spec}(A)$ and $Z = \mathrm{Spec}(B)$ and where φ comes from some homomorphism $\psi : B \longrightarrow A$. We may further assume that f has exactly one zero or pole on Z, say at z, and that there is exactly one $y \in Y$ lying over z.

In this situation, i restricts to give a map $\mathcal{O}_{Z,z} \longrightarrow \mathcal{O}_{Y,y}$. This map is ramified of degree $e(y)$, which means:

$$v_y((\tilde{f})) = v_y(i(f)) = e(y) \cdot (v_z(f))$$

This suffices to prove the claim. □

4.2. **Push forwards.**

Definition 4.4. The **degree**, $\deg(\varphi)$, of the morphism φ is the degree of the field extension $\mathcal{K}(Y) \supset \mathcal{K}(Z)$. This number is finite because φ is finite by assumption.

Definition 4.5. We define the **push forward** of a divisor $D \in \mathrm{Div}(Y)$ by defining it for prime divisors and extending linearly. For D a prime divisor on Y, we let $\varphi_*(D) = 0$ if $\varphi(D)$ codimension greater than 1 in Y and $\varphi_*(D) = \deg(\varphi|_D) \cdot \varphi(D)$ if $\varphi(D)$ has codimension one. In a different language, for $D = [y]$ and $z = \varphi(y)$, we let $\varphi_*(D) = 0$ if z has codimension greater than 1 and $\varphi_*(D) = [\Bbbk_z : \Bbbk_y][z]$ if z has codimension 1.

[1] This means that $\dim \overline{\{y\}} = \dim Y - 1$, where $\overline{\{y\}}$ is the closure of y in Y.

[2] Recall that normal schemes are in particular nonsingular in codimension 1.

The constant in this definition is justified by the corollary to the following proposition.

Proposition 4.6. *For $g \in \mathcal{K}(Y)$, we have $\varphi_*((g)) = (N_{\mathcal{K}(Y)/\mathcal{K}(Z)}(g))$, where $N_{\mathcal{K}(Y)/\mathcal{K}(Z)} : \mathcal{K}(Y) \longrightarrow \mathcal{K}(Z)$ denotes the norm map.*

Corollary 4.7. *Push forwards preserve linear equivalence and therefore descend to give a map $\mathrm{Pic}(Y) \longrightarrow \mathrm{Pic}(Z)$.*

Proof. That the corollary follows from the proposition is clear.

To prove the proposition, we will need the following lemma.

Lemma 4.8. *Let $A \subset B$ be Dedekind domains with B finite as an A-module and with fields of fractions $K \subset L$. For a prime $\mathfrak{p} \subset A$, let $B\mathfrak{p} = \prod \mathfrak{q}^{e(\mathfrak{q})}$ be the factorization of $B\mathfrak{p}$ into primes of B. Let $f(\mathfrak{q}) = [B/\mathfrak{q} : A/\mathfrak{p}]$. Then $\sum e(\mathfrak{q})f(\mathfrak{q}) = [L : K]$.*

Proof. By localizing at $A \setminus \mathfrak{p}$, we may assume A to be a DVR. Then because A is a PID and B is a finitely generated, torsion free A-module, it is free of rank $[L : K]$. Thus, $\dim_{A/\mathfrak{p}}(B/\mathfrak{p}B) = [L : K]$. By the Chinese remainder theorem, the following map is a surjection:

$$B/\mathfrak{p}B \longrightarrow \prod B/\mathfrak{q}^{e(\mathfrak{q})}$$

Thus, comparing the dimensions of both sides over $A/\mathfrak{p}$, we get:

$$[L : K] = \sum \dim_{A/\mathfrak{p}}(B/\mathfrak{q}^{e(\mathfrak{q})})$$

However, because as $A/\mathfrak{p}$-modules $B/\mathfrak{q}^{e(\mathfrak{q})} \cong (B/\mathfrak{q})^{\oplus e(\mathfrak{q})}$, we have $\dim_{A/\mathfrak{p}}(B/\mathfrak{q}^{e(\mathfrak{q})}) = e(\mathfrak{q})f(\mathfrak{q})$. □

We proceed on the proposition by a series of reductions. First we may immediately reduce to the affine case where $Y = \mathrm{Spec}(B)$ and $Z = \mathrm{Spec}(A)$ for B a finite A-algebra and where A and B are domains regular in codimension 1, say with fields of fractions K and L respectively. We may suppose further that all zeros and poles lie above one prime $\mathfrak{p} \in \mathrm{Spec}(A)$, say at $\{\mathfrak{q}\} \subset \mathrm{Spec}(B)$. We then get a map between $A_\mathfrak{p} \longrightarrow B_{A\setminus\mathfrak{p}}$ where now $B_{A\setminus\mathfrak{p}}$ must be finite as an $A_\mathfrak{p}$-module as it is a finite algebra over a DVR. Therefore, $B_{A\setminus\mathfrak{p}} = B'$ is a Dedekind domain. In the notation of Lemma 4.8, we have $\deg(\varphi|_{[\mathfrak{q}]}) = f(\mathfrak{q})$. We need to show that, where $g \in L^*$:

$$\sum_\mathfrak{q} f(\mathfrak{q})v_\mathfrak{q}(g) = v_\mathfrak{p}(N_{L/K}(g)) \qquad (*)$$

By Lemma 4.8, $\displaystyle\sum_\mathfrak{q} e(\mathfrak{q})f(\mathfrak{q}) = [L : K]$.

Consider the case where $g \in K^*$ so that $v_\mathfrak{q}(g) = e(\mathfrak{q})v_\mathfrak{p}(g)$ and $N_{L/K}(g) = g^{[L:K]}$. Thus:

$$v_\mathfrak{p}(N_{L/K}(g)) = v_\mathfrak{p}(g^{[L:K]}) = [L : K]v_\mathfrak{p}(g) = \sum_\mathfrak{q} e(\mathfrak{q})f(\mathfrak{q})v_\mathfrak{p}(g) = \sum_\mathfrak{q} f(\mathfrak{q})v_\mathfrak{q}(g).$$

Furthermore, notice that because both sides of $(*)$ take powers to sums, if the result is true for some power of g then it is true for g. Thus, if L/K is purely inseparable, the result follows.

We now wish to reduce to the case of a separable extension. Because every extension is the composition of a purely inseparable extension and a separable extension, it suffices to show that if the result holds for an extension E/K and for L/E, then it follows for L/K. For notational reasons, this is somewhat easier to show for schemes than for rings. Let W be the normalization of Y in E, so that φ factors through:

$$Y \xrightarrow{\alpha} W \xrightarrow{\beta} Z$$

The computation is now clear, noting that the functorality of push forwards follow directly from the definition:

$$\begin{aligned}(\beta \circ \alpha)_*((g)) = \beta_*(\alpha_*((g))) &= \beta_*((N_{K(Y)/K(W)}(g)) \\ &= (N_{K(W)/K(Z)}(N_{K(Y)/K(W)}(g))) \\ &= (N_{K(Y)/K(Z)}(g)).\end{aligned}$$

Next, we wish to reduce to the case where the extension is Galois. This however, is clear because $K \subset L$ is contained in a finite Galois extension $K \subset L \subset M$. The statement follows from an identical argument because it is true for $L \subset M$ and for $K \subset M$.

By [Se79] §1.7, the group $G = \mathrm{Gal}(L/K)$ acts transitively on the set $\{\mathfrak{q}\}$ of primes of B' lying over $\mathfrak{p}$. Fix one of them, say $\mathfrak{q}_0$. Then if $\sigma \cdot \mathfrak{q}_0 = \mathfrak{q}$ for $\sigma \in G$, we have:

$$v_{\mathfrak{q}_0}(g) = v_{\sigma \cdot \mathfrak{q}_0}(\sigma \cdot g) = v_{\mathfrak{q}}(\sigma \cdot g)$$

Therefore:

$$\begin{aligned}\sum_{\mathfrak{q}} f(\mathfrak{q}) v_{\mathfrak{q}}(g) &= \frac{1}{|\mathrm{stab}(\mathfrak{q}_0)|} \sum_{\sigma \in G} f(\sigma \cdot \mathfrak{q}_0) v_{\sigma \cdot \mathfrak{q}_0}(g) \\ &= \frac{f(\mathfrak{q}_0)}{|\mathrm{stab}(\mathfrak{q}_0)|} \sum_{\sigma \in G} v_{\mathfrak{q}_0}(\sigma \cdot g) \\ &= \frac{f(\mathfrak{q}_0)}{|\mathrm{stab}(\mathfrak{q}_0)|} v_{\mathfrak{q}_0}(N_{L/K}(g)) \\ &= \frac{f(\mathfrak{q}_0) e(\mathfrak{q}_0)}{|\mathrm{stab}(\mathfrak{q}_0)|} v_{\mathfrak{p}}(N_{L/K})\end{aligned}$$

The result now follows as, because as the extension is Galois:

$$|G| = |L : K| = \sum_{\mathfrak{q}} e(\mathfrak{q}) f(\mathfrak{q}) = \frac{|G|}{|\mathrm{stab}(\mathfrak{q}_0)|} e(\mathfrak{q}_0) f(\mathfrak{q}_0).$$

□

Combining φ_* and φ^* gives us endomorphisms of $\mathrm{Div}(Y)$ and $\mathrm{Div}(Z)$. The endomorphism of $\mathrm{Div}(Y)$ is difficult to describe, but that of $\mathrm{Div}(Z)$ admits a very simple description.

Proposition 4.9. *The endomorphism $\varphi_*\varphi^*$ of $\mathrm{Div}(Z)$ acts by $D \mapsto \deg(\varphi) \cdot D$.*

Proof. Suppose z is a codimension 1 point of Z. Then:

$$\varphi_*\varphi^*([z]) = \sum_{\varphi(y)=z} e(y) \deg(\varphi|_{[y]}) \cdot [z] = e(y)f(y) \cdot [z] = \deg(\varphi) \cdot [z]$$

□

5. Intersection theory on surfaces

We will require throughout this section that $\Bbbk$ be an algebraically closed field.

5.1. **Relationship to cohomology.** Before discussing intersection theory, we will describe why it is the natural place to look for a set of tools. The thought of the Grothendieck school was that the Weil conjectures would yield under the development of appropriate cohomological techniques on algebraic varieties because their analogues for Kähler manifolds could be proved by some basic facts about their cohomological structure. This led to the development of étale cohomology which was able to prove the first two conjectures. However, that étale cohomology seemed not powerful enough to prove the Riemann hypothesis for varieties led Grothendieck to initiate the theory of motives with their "standard conjectures" which, if proven, would give a conceptual proof of the last Weil conjecture.

Intersection theory reflects something of the cohomological structure of a variety. This is because it deals in general with algebraic cycles, though we will be concerned only with divisors, which are the appropriate analogues of cycles of classical topology.

5.2. **Basic definitions.** We wish to find a definition of the intersection number of two closed[3] curves on a smooth, projective surface Y, with the intention of eventually applying our techniques to the particular surface $Y = X \times_{\mathrm{Spec}(\overline{\mathbb{F}_q})} X$. We may immediately extend any such map to $\mathrm{Div}(Y) \times \mathrm{Div}(Y) \longrightarrow \mathbb{Z}$ by linearity. We want a map which is symmetric, invariant under linear equivalence and which accounts for "multiplicity." We say two smooth curves intersect "transversely" at a point if their tangent spaces sum to give the tangent space of the surface at that point. This will give our conception of two curves intersecting with multiplicity one. To account for higher multiplicity, we intuitively want to say that intersection numbers are invariant under slight perturbation. This notion would say, for example, that the parabolas $y = x^2$ and $y = -x^2$ have intersection number 2 because if we slightly perturbed them they would intersect transversely in two places.

[3]We will assume without further mention that all curves with which we deal are closed.

Definition 5.1. Two smooth curves C and D intersect **transversely** at $P \in Y$ if, there are regular functions f and g defined in a neighborhood of P in Y, so that C is given locally near P as the zeros of f and D by g, and such that the images of f and g generate the maximal ideal of $\mathcal{O}_{Y,P}$. We simply say that C and D intersect **transversely** if they do so at every point of their intersection.

Remark 5.2. The reader familiar with tangent spaces on algebraic varieties will immediately recognize that this definition is exactly equivalent to the situation described above.

Proposition 5.3. *If C and D intersect transversely, then* $\deg_C(\mathcal{O}(D)|_C) = \#(C \cap D)$.

Proof. We may clearly assume that C and D are connected. Since they are smooth by assumption, it follows that they are irreducible. We will write $\mathcal{O}_{Y,D}$ for the local ring of Y at the generic point of D. In other words, $\mathcal{O}_{Y,D}$ is the ring of rational functions on Y whose only poles are along the divisor D.

Let P be an intersection point of C and D and let f and g be as in Definition 5.1, so that in particular f is a uniformizer in $\mathcal{O}_{Y,D}$. We have the maps:

$$\mathcal{O}_{Y,D} \longrightarrow \mathcal{O}_{Y,P} \longrightarrow \mathcal{O}_{C,P}$$

We claim that the image of f under these maps generates the maximal ideal of $\mathcal{O}_{C,P}$. Consider the following short exact sequence, where $\mathfrak{I}_C$ is the ideal sheaf of C in Y:

$$0 \longrightarrow \mathfrak{I}_{C,P} \longrightarrow \mathcal{O}_{Y,P} \longrightarrow \mathcal{O}_{C,P} \longrightarrow 0$$

By the transversality assumption, f and g generate the maximal ideal of $\mathcal{O}_{Y,P}$, therefore, their images generate the maximal ideal of the quotient $\mathcal{O}_{C,P}$. However, as g is killed by this quotient, it must be that the image of f generates this maximal ideal.

This is exactly to say that a uniformizer in $\mathcal{O}_{Y,D}$ is sent to a uniformizer in $\mathcal{O}_{C,P}$. In other words, the $\Bbbk$-dimension of the stalk of the quotient $\mathcal{O}_C/\left(\mathcal{O}(-D)\big|_C\right)$ at P equals 1. Since this quotient is supported precisely at the intersection points of C and D, it follows that $\deg_C(\mathcal{O}(D)|_C) = \sum_{P \in C \cap D} 1 = \#(C \cap D)$. □

Corollary 5.4. *If D and D' are irreducible curves intersecting whose prime divisors are linearly equivalent and which intersect C transversely, then $\#(C \cap D) = \#(C \cap D')$.*

Proof. This follows because $\mathcal{O}(D) \cong \mathcal{O}(D')$. □

Definition 5.5. For C a smooth curve on Y and $D \in \mathrm{Div}(Y)$, the **intersection number** of C with D is $(C.D) = \deg(\mathcal{O}_Y(D)|_C)$.

Proposition 5.6. *With χ denoting the Euler characteristic,* $(C.D) = \chi(\mathcal{O}_Y(D)|_C) - \chi(\mathcal{O}_C) = \chi(\mathcal{O}_C) - \chi(\mathcal{O}_Y(-D)|_C)$

Proof. By Riemann-Roch, for any line bundle $\mathscr{L}$ on a smooth projective curve C:

$$\chi(\mathscr{L}) = \deg(\mathscr{L}) + 1 - g(C) = \deg(\mathscr{L}) + \chi(\mathcal{O}_C)$$

Let $\mathscr{L} = \mathcal{O}_Y(D)$ and $\mathscr{L} = \mathcal{O}_Y(-D)$ to obtain these results, noting that $\deg(\mathcal{O}_Y(D)) = -\deg(\mathcal{O}_Y(-D))$. □

This is useful because it gives us a workable definition for any possibly singular curve C.

Definition 5.7. For C a not necessarily smooth curve on Y and $D \in \mathrm{Div}(Y)$, the **intersection number** of C with D is $(C.D) = \chi(\mathcal{O}_Y(D)|_C) - \chi(\mathcal{O}_C) = \chi(\mathcal{O}_C) - \chi(\mathcal{O}_Y(-D)|_C)$. We may extend this definition by linearity to give the definition of intersection number for any two divisors on Y.

Theorem 5.8. *For any two divisors $C, D \in \mathrm{Div}(Y)$, $(C.D) = \chi(\mathcal{O}_Y) - \chi(\mathcal{O}_Y(-C)) - \chi(\mathcal{O}_Y(-D)) + \chi(\mathcal{O}_Y(-C-D))$.*

Proof. First, consider the case where C is a curve. Then we have the short exact sequence, because the functions killed by the restriction map are exactly those with a zero along C:

$$0 \longrightarrow \mathcal{O}_Y(-C) \longrightarrow \mathcal{O}_Y \longrightarrow \mathcal{O}_C \longrightarrow 0$$

Because $\mathcal{O}(-D)$ is a line bundle, it is a flat $\mathcal{O}_Y$ module (because flatness is a local property and $\mathcal{O}_Y|_U$ is clearly flat). Thus, tensoring with $\mathcal{O}(-D)$ we see that the following sequence is also exact:

$$0 \longrightarrow \mathcal{O}_Y(-C-D) \longrightarrow \mathcal{O}_Y(-D) \longrightarrow \mathcal{O}(-D)|_C \longrightarrow 0$$

Together, these imply:

$$\chi(\mathcal{O}_Y) - \chi(\mathcal{O}_Y(-C)) - \chi(\mathcal{O}_Y(-D)) + \chi(\mathcal{O}_Y(-C-D)) = \chi(\mathcal{O}_C) - \chi(\mathcal{O}_Y(-D)|_C) = (C.D)$$

With this, it now suffices to show that the map $(C, D) \mapsto \chi(\mathcal{O}_Y) - \chi(\mathcal{O}_Y(-C)) - \chi(\mathcal{O}_Y(-D)) + \chi(\mathcal{O}_Y(-C-D))$ is bilinear. We merely sketch this proof because it requires the use of ample sheaves and a full discussion of them would be too much of a digression. The reader is referred to [Mu66] for the necessary details. By Bertini's theorem, every divisor on Y is linearly equivalent to the difference of two smooth curves. Therefore, we are reduced to the case as described in Definition 5.5, at which point it is true because it is bilinear with respect to D simply because the degree map is a homomorphism, and then our claim follows because the intersection form is symmetric. □

5.3. **The Néron-Severi group.** In fact, the intersection form immediately gives us a useful equivalence relation that is weaker than linear equivalence.

Definition 5.9. We say that two divisors are **numerically equivalent** if their intersection numbers with any third divisor are equal. We define the **Néron-Severi group** of Y to be $\mathrm{NS}(Y) = \mathrm{Div}(Y)/\{\text{divisors numerically equivalent to } 0\}$.

Note that the intersection form descends to give a nondegenerate symmetric bilinear form $\mathrm{NS}(Y) \times \mathrm{NS}(Y) \longrightarrow \mathbb{Z}$. In particular, $\mathrm{NS}(Y)$ is a torsion-free abelian group. This group is in fact finitely generated as in proved in [LN59]. However, we will not need this result.

5.4. **Relationship to §4.**

Proposition 5.10. *For $C \in \mathrm{Div}(Y)$ and $D \in \mathrm{Div}(Z)$, $(C.\varphi^*(D)) = (\varphi_*(C).D)$.*

Proof. Again, by Bertini's theorem we may assume by bilinearity that C and D are smooth, prime divisors. In this case it is clear because we may compute:

$$\begin{aligned}(\varphi^*C.D) = \deg(\mathcal{O}(\varphi^*C)|_D) &= \deg((\varphi^*\mathcal{O}(C))|_D) \\ &= \deg(\varphi^*\mathcal{O}(C)|_{\varphi(D)}) \\ &= \deg(\varphi|_D)\cdot\deg(\mathcal{O}(C)|_{\varphi(D)}) \\ &= (\varphi_*(C).D)\end{aligned}$$

□

6. Proof of the Riemann Hypothesis for curves

We return now to the Weil conjectures for curves over finite fields. Let us reinstate the hypotheses and notation of §2. Let us also dictate that $Y = X \times_{\mathrm{Spec}(\overline{\mathbb{F}_q})} X$. We will first set up the absolute Frobenius morphism on X then give the last results we need before proving the Riemann hypothesis for X_0.

6.1. **The Frobenius morphisms.** For A any $\mathbb{F}_q$-algebra, let $\varphi : A \longrightarrow A$ be the Frobenius substitution, that is, the homomorphism $a \mapsto a^q$. Then φ gives us a morphism $\Phi_{X_0} : X_0 \longrightarrow X_0$ in the following manner: on the level of topological spaces, let Φ_{X_0} be the identity map and then for any open $U \subset X_0$ define $\Phi^*_{X_0}(U) = \varphi$.

Definition 6.1. This morphism of schemes is the **absolute Frobenius morphism** on X_0. Its extension $\mathrm{Fr}_X = \Phi_{X_0} \times \mathrm{id}$ to X is the **Frobenius endomorphism** of X.

Remark 6.2. The absolute Frobenius morphism is defined functorially among schemes over $\mathbb{F}_q$. That is, given any morphism $\psi : X_0 \longrightarrow Y_0$, we have $\psi \circ \Phi_{X_0} = \Phi_{Y_0} \circ \psi$.

Note that $X(\overline{\mathbb{F}_q}) = X_0(\overline{\mathbb{F}_q})$ straight from the universal property defining X. These two sets have two natural Frobenius actions on them, namely, $X(\overline{\mathbb{F}_q})$ has the action given by the Frobenius endomorphism and $X_0(\overline{\mathbb{F}_q})$ has the action induced by the Galois action as $\varphi^* : \mathrm{Spec}(\overline{\mathbb{F}_q}) \longrightarrow \mathrm{Spec}(\overline{\mathbb{F}_q})$ is a morphism of schemes over $\mathbb{F}_q$.

Proposition 6.3. *These two actions are identical.*

Proof. As $\varphi^* = \Phi_{\mathrm{Spec}(\overline{\mathbb{F}_q})}$, by Remark 6.2 we have for all $x \in \mathrm{Hom}_{\mathbb{F}_q - sch}(\mathrm{Spec}(\overline{\mathbb{F}_q}), X_0)$:

$$(x \circ \varphi^*) \times \mathrm{id} = (x \circ \Phi_{\mathrm{Spec}(\overline{\mathbb{F}_q})}) \times \mathrm{id} = (\Phi_{X_0} \circ x) \times \mathrm{id} = \mathrm{Fr}_X \circ (x \times \mathrm{id}).$$

□

6.2. **Preparatory results.** Let Δ_X and $\Gamma_{\mathrm{Fr}_X^n}$ denote the graphs of the diagonal morphism and Fr_X^n respectively in Y.

Lemma 6.4. *We have* $[\Gamma_{\mathrm{Fr}_X^n}] = ((\mathrm{Fr}_X \times \mathrm{id}_X)^*)^n[\Delta_X]$.

Proof. Note first by functorality of pull backs we have $((\mathrm{Fr}_X \times \mathrm{id}_X)^*)^n = (\mathrm{Fr}_X^n \times \mathrm{id}_X)^*$. Thus, it suffices to show that for an arbitrary endomorphism $\psi : X \longrightarrow X$, we have $[\Gamma_\psi] = (\psi \times \mathrm{id}_X)^*[\Delta_X]$, where Γ_ψ is the graph of ψ in Y.

It suffices to prove this locally, so assume that $X = \mathrm{Spec}(A)$. Consider a closed point $x \in X$ and take π a uniformizer in $\mathcal{O}_{X,x}$. We may assume π comes from a global section, that is, $\pi \in A$. By pulling back π along each of the two projections, we get two sections π_1 and π_2 of Y. Then $\pi_1 - \pi_2 \in \Gamma(Y, \mathcal{O}_Y)$ generates the ideal of Δ_X. Pulling back along $\psi \times \mathrm{id}$ takes $\pi_1 - \pi_2$ to $\psi^*(\pi_1) - \pi_2$. However, this clearly generates the ideal of Γ_ψ. □

Lemma 6.5. *For all* $n \in \mathbb{N}$*, we have* $([\Gamma_{\mathrm{Fr}_X^n}].[\Delta_X]) = |X(\mathbb{F}_{q^n})|$.

Proof. Because Fr_X^n has vanishing differential, $\Gamma_{\mathrm{Fr}_X^n}$ and Δ_X meet transversely at every point. Furthermore, they must meet only at closed points because they are both irreducible of dimension 1. Thus, it suffices to show that the number of closed points where they intersect is equal to $|X(\mathbb{F}_{q^n})|$. Because we are dealing only with closed points and schemes of finite type, by the Nullstellensatz the closed points of Y is just the set theoretic product of closed points of X with itself. At this point the result is clear because $\mathrm{Fr}_X^n(x) = x$ if and only if x is fixed by $(\varphi^*)^n$ by Proposition 6.3. □

We will also need the Hodge index theorem to proceed. The reader is referred to [Mu66], §18 for a proof. We recall the statement of the theorem:

Theorem 6.6. *The intersection form has index 1 on* $\mathrm{NS}(Y)$*, that is, we have an internal direct sum decomposition* $\mathrm{NS}(Y) \otimes_{\mathbb{Z}} \mathbb{Q} = V \oplus V'$*, such that* V *has dimension* 1 *and the intersection form is positive definite on* V *and negative definite on* V'*.*

6.3. **The Riemann hypothesis.** We now have all the tools we will need at hand.

Lemma 6.7. *We have* $|X(\mathbb{F}_{q^n})| = q^n + O(q^{\frac{n}{2}})$.

Proof. Let W be the $\mathbb{Q}$-vector space $\mathrm{NS}(Y) \otimes_{\mathbb{Z}} \mathbb{Q}$. We have a nondegenerate symmetric bilinear form $(\cdot, \cdot)$ on W inherited by the intersection form. By Theorem 6.6, it is positive definite on a vector space of dimension exactly 1.

Let $[H]$ and $[V]$ be the divisors corresponding to the horizontal and vertical axes in $X \times X$, that is, $X \times \{x_0\}$ and $\{x_0\} \times X$ for some chosen closed point x_0 of X. These are not equal in $\mathrm{NS}(Y)$ because $([H].[V]) = 1$ and $([H].[H]) = 0$. Therefore, if $U = \mathbb{Q}[H] \oplus \mathbb{Q}[V]$ we get a decomposition $W = U \oplus U'$ where U' is the orthogonal complement to U because U is finite dimensional. We claim that the bilinear form is negative definite on U'. Its matrix on U with respect to the basis $\{[H], [V]\}$ equals:

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

This matrix has one positive eigenvalue, so the subspace on which $(\cdot,\cdot)$ is positive definite is contained in U and therefore U' is contained in its orthogonal complement, on which $(\cdot,\cdot)$ is negative definite.

Let $T : W \longrightarrow W$ be the linear transformation $D \longmapsto (\mathrm{Fr}_X \times \mathrm{id}_X)^* D$. Then $T[H] = q \cdot [H]$ and $T[V] = [V]$ as follows immediately from the definition of pull backs. We know by Lemma 6.4 that $T^n[\Delta_X] = [\Gamma_{\mathrm{Fr}_X^n}]$. Furthermore, because $\deg(\mathrm{Fr}_X \times \mathrm{id}_X) = q$, by Propositions 5.10 and 4.9, we have that for all $D, E \in \mathrm{NS}(Y)$:

$$((\mathrm{Fr}_X \times \mathrm{id}_X)^* D.(\mathrm{Fr}_X \times \mathrm{id}_X)^* E) = (D.(\mathrm{Fr}_X \times \mathrm{id}_X)_*(\mathrm{Fr}_X \times \mathrm{id}_X)^* E) = (D.qE) = q \cdot (D.E)$$

Thus, for all $v, w \in W$, $(Tv, Tw) = q(v, w)$.

Let us set $\Delta_X = u + u'$ for $u = [H] + [V] \in U$, $u' \in U'$, and we then compute:

$$\begin{aligned} |X(\mathbb{F}_{q^n})| = ([\Gamma_{\mathrm{Fr}_X^n}].[\Delta_X]) &= (T^n \Delta_X, \Delta_X) \\ &= (T^n([H] + [V] + u'), [H] + [V] + u') \\ &= q^n + 1 + (T^n u', u') \end{aligned}$$

However, because $(\cdot,\cdot)$ is negative definite on U', we may apply the Cauchy-Schwarz inequality to see that:

$$|(T^n u', u')| \leq \sqrt{|(T^n u', T^n u')||(u', u')|} = \sqrt{q^n |(u', u')|} = O(q^{n/2})$$

□

By Proposition 3.2, this suffices to show the Riemann hypothesis for curves.

References

[AK70] A. Altman and S. Kleiman, "Introduction to Grothendieck duality theory," Lecture Notes in Math. **146**, Springer-Verlag, Berlin–New York, 1970.

[Bo74] E. Bombieri, *Counting points on curves over finite fields* (*d'après S. A. Stepanov*), Séminaire Bourbaki, 25ème année (1972/1973), Exp. No. 430, pp. 234–241. Lecture Notes in Math. **383**, Springer, Berlin, 1974.

[De74] P. Deligne, *La conjecture de Weil I*, Publ. Math. IHES **43** (1974), 273–307.

[Dw60] B. Dwork, *On the rationality of the zeta function of an algebraic variety*, Amer. J. Math. **82** (1960), 631–648.

[Gr64] A. Grothendieck, *Formule de Lefschetz et rationalité des fonctions L*, Séminaire Bourbaki **9** (Déc. 1964), Exp. No. 279, pp. 41–55, Soc. Math. France, Paris, 1995.

[Mu66] D. Mumford, "Lectures on curves on an algebraic surface," Annals of Mathematics Studies **59**, Princeton University Press, Princeton, NJ, 1966.

[LN59] S. Lang and A. Néron, *Rational points of abelian varieties over function fields*, Amer. J. Math. **81** (1959), 95–118.

[Se79] J. P. Serre, "Local fields," Graduate Texts in Math. **67**, Springer-Verlag, New York-Berlin, 1979.

[St69] S. A. Stepanov, *The number of points of a hyperelliptic curve over a finite prime field*, Izv. Akad. Nauk SSSR Ser. Mat. **33**, 1969, 1171–1181.

[We48] A. Weil, "Sur les courbes algébriques et les variétés qui s'en déduisent," Actualités Sci. Ind. **1041** = Publ. Inst. Math. Univ. Strasbourg **7** (1945). Hermann et Cie., Paris, 1948.

[We49] A. Weil, *Numbers of solutions of equations in finite fields*, Bull. AMS **55** (1949), 497–508.