21. Lecture 21 (Apr 21 & 23): Point counting over finite fields

In the final part of the course, we shall apply the theory we have developed to an arithmetic problem: the Riemann hypothesis for curves over finite fields.

Recommended reading:

- Hartshorne [Har77, Appendix C];
- notes by Sam Raskin[1];
- the book [Lor96] *An Invitation to Arithmetic Geometry* by Dino Lorenzini (Chapters VIII and X).

The Weil conjectures for curves can also be deduced from the inequalities for correspondences in Kempf [Kem93, §10.8] (his proof does not require intersection theory on surfaces).

21.1. Varieties over non-closed fields and rational points

The formalism of algebraic varieties developed in this course is not so well equipped to deal with geometry over fields which are not algebraically closed, since a variety over a field might not have any points with coordinates that field (e.g. $V(x^2+y^2+1)$ over $\mathbb{R}$). This is one more reason to use schemes, which work well over arbitrary base fields (or even over rings such as $\mathbb{Z}$). Instead of doing that, we circumvent the difficulties by fixing an embedding into an affine or projective space; this is a bit cumbersome, but will do for our purposes.

Definition 21.1.1. Let k be an algebraically closed field and let $k_0 \subseteq k$ be a subfield. We say that a closed subset X of $\mathbb{A}^n$ is **defined over** k_0 if there exist polynomials $f_1,\dots,f_r \in k_0[T_1,\dots,T_n]$ such that $X = V(f_1,\dots,f_r)$. A point $x \in X$ is **rational over** k_0 if it is defined over k_0, or equivalently if $x = (x_1,\dots,x_n)$ where $x_1,\dots,x_n \in k_0$. We write $X(k_0)$ for the set of all $x \in X$ which are rational over k_0. We make the same definitions for $X \subseteq \mathbb{P}^n$ (in which case $f_1,\dots,f_r \in k_0[T_0,\dots,T_n]$ are supposed to be homogeneous).

Remark 21.1.2.

1. Obviously, being defined over k_0 depends on the embedding (already if X is a point). To see how to get a reasonable "hands-on" theory of varieties over k_0 using algebraic varieties over k, see [Mum99, §II.4].
2. This definition has many variants. For example, we could extend it to locally closed (or constructible) subsets. If X is a variety, we can define "divisors on X defined over k_0." A map $f\colon Y \to X$ between two varieties defined over k_0 (with respect to a pair of embeddings a projective spaces) is defined over k_0 if its graph (embedded using the Segre embedding) is defined over k_0, and so on.

21.2. The Hasse–Weil zeta function

The Riemann zeta function $\zeta(s)$ of the complex variable s (with $\mathrm{Re}(s) > 1$) is

$$\zeta(s) = \sum_{n\geq 1} n^{-s} = \prod_p \frac{1}{1-p^{-s}}.$$

This equality (the "Euler product") is an analytic avatar of unique factorization of positive integers as products of powers of primes. It extends to a meromorphic function on the complex plane with a single

[1] https://math.uchicago.edu/~may/VIGRE/VIGRE2007/REUPapers/FINALFULL/Raskin.pdf

pole at zero, and the **Riemann hypothesis** is the conjecture that the zeros of $\zeta(s)$ in the "critical strip" $0 \leq \mathrm{Re}(s) \leq 1$ lie on the line $\mathrm{Re}(s) = 1/2$. This statement has many equivalent forms, often stated in terms of the asymptotics of the prime counting function $\pi(x)$.

We now build an analog of the Riemann zeta function associated to a variety defined over a finite field. In fact, this is more than an analogy, as Remark 21.3.5 will explain why both are special cases of a more general construction. For this, we need to recall a few **facts about finite fields**. Let $\mathbb{F}_q$ be a finite field of cardinality $q = p^c$ and let $\overline{\mathbb{F}}_q = \overline{\mathbb{F}}_p$ be a fixed algebraic closure. We can identify $\mathbb{F}_q$ as the set of solutions of $T^q - T = 0$ inside $\overline{\mathbb{F}}_q$. More generally, for every $r \geq 1$, we the set $\mathbb{F}_{q^r}$ of solutions of $T^{q^r} - T = 0$ is the unique extension of $\mathbb{F}_q$ of degree r (and hence a field of cardinality q^r). The Galois group $\mathrm{Gal}(\mathbb{F}_{q^r}/\mathbb{F}_q)$ is cyclic of order r, generated by the Frobenius automorphism $x \mapsto x^q$.

From now on we work in our usual algebraic geometry framework over the algebraically closed field $k = \overline{\mathbb{F}}_q$, so for example $\mathbb{P}^n$ denotes the projective n-space over $k = \overline{\mathbb{F}}_q$. We use the terminology introduced in §21.1: a locally closed $X \subseteq \mathbb{P}^n$ is defined over $\mathbb{F}_q$ if it is defined using homogeneous polynomials with coefficents in $\mathbb{F}_q$, and a point $x \in X$ is rational over $\mathbb{F}_q$ if $x = (x_0 : \cdots : x_n)$ with $x_i \in \mathbb{F}_q$, or equivalently if $\{x\}$ is defined over $\mathbb{F}_q$. We write

$$X(\mathbb{F}_q) = \{x \in X : x \text{ is defined over } \mathbb{F}_q\}.$$

Since $\mathbb{F}_q$ is finite, this is a finite set. Obviously if X is defined over $\mathbb{F}_q$, it is also defined over $\mathbb{F}_{q^r}$ for all $r \geq 1$, and so the notation $X(\mathbb{F}_{q^r})$ makes sense. Since every point is defined over *some* finite extension of $\mathbb{F}_q$, we have

$$X = \bigcup_{r \geq 1} X(\mathbb{F}_{q^r}).$$

The basic questions we aim to answer are:

How big is the set $X(\mathbb{F}_q)$? *How fast does the size of $X(\mathbb{F}_{q^r})$ grow with r?*

It is convenient to pack the numbers $\#X(\mathbb{F}_{q^r})$ into a kind of generating function.

Definition 21.2.1. Let $X \subseteq \mathbb{P}^n$ be a locally closed subset defined over $\mathbb{F}_q$. The **Hasse–Weil zeta function** of X over $\mathbb{F}_q$ is the formal power series

$$Z(X/\mathbb{F}_q, T) = \exp\left(\sum_{r=1}^{\infty} \frac{\#X(\mathbb{F}_{q^r})}{r} T^r\right) \quad \in \quad \mathbb{Q}[\![T]\!].$$

A nice property of the zeta function is that it can be computed "piece by piece."

Remark 21.2.2 (Scissor relations)**.** If X is the disjoint union of locally closed subsets X_1 and X_2, then $\#X(\mathbb{F}_{q^r}) = \#X_1(\mathbb{F}_{q^r}) + \#X_2(\mathbb{F}_{q^r})$ and consequently

$$Z(X/\mathbb{F}_q, T) = Z(X_1/\mathbb{F}_q, T) \cdot Z(X_2/\mathbb{F}_q, T).$$

In the example below, and many times afterwards, we shall use the power series expansion

$$\log\left(\frac{1}{1-\alpha T}\right) = \sum_{r \geq 1} \frac{\alpha^r}{r} T^r. \tag{21.2.1}$$

Example 21.2.3 (Projective space)**.** Let $X = \mathbb{P}^n$, then we can write

$$X = \mathbb{A}^n \sqcup \mathbb{A}^{n-1} \sqcup \cdots \sqcup \mathbb{A}^0,$$

and using the scissor relations we get

$$\#X(\mathbb{F}_{q^r}) = 1 + q^r + \cdots + q^{rn}.$$

Using (21.2.1) we turn this to

$$Z(\mathbb{P}^n/\mathbb{F}_q, T) = \frac{1}{(1-T)(1-qT)\dots(1-q^nT)}.$$

Example 21.2.4 (Fermat curves)**.** For $d \geq 1$ prime to p, consider the Fermat curve

$$X_d = \{x^d + y^d + z^d = 0\} \subseteq \mathbb{P}^2.$$

Let $q = p^c$ be such that $q = 1$ modulo d. Obviously X_d is defined over $\mathbb{F}_p$ and hence over $\mathbb{F}_q$. According to the rather ingenious computation in [IR90, §11.3], we have

$$Z(X_d/\mathbb{F}_q, T) = \frac{\prod_{\alpha\beta\gamma=1}\left(1 + \frac{g(\alpha)g(\beta)g(\gamma)}{q}T\right)}{(1-T)(1-qT)},$$

the product taken over triples of non-trivial characters

$$\alpha, \beta, \gamma \colon \mathbb{F}_q^\times \longrightarrow \mu_d(\mathbb{C})$$

valued in d-th order roots of unity satisfying the equality $\alpha\beta\gamma = 1$. The degree of the numerator equals $(d-1)(d-2)$, which coincides with $2g$ where g is the genus of X_d. Here for a character $\chi \colon \mathbb{F}_q^\times \to \mathbb{C}^\times$, the $g(\chi)$ denotes the **Gauss sum**

$$g(\chi) = \sum_{x \in \mathbb{F}_q^\times} \chi(x) \exp\left(\frac{2\pi i \cdot \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(x)}{p}\right).$$

A key property of the Gauss sum is that $|g(\chi)| = q^{1/2}$ for $\chi \neq 1$. It follows that the $2g$ roots of $Z(X_d/\mathbb{F}_q, T)$ have absolute value $q^{-1/2}$.

21.3. The Weil conjectures

The goal of the lecture is to prove the following result, generalizing the explicit computation for the Fermat curve in Example 21.2.4.

Theorem 21.3.1 (Hasse–Schmidt–Weil, "Weil conjectures for curves")**.** *Let $X \subseteq \mathbb{P}^n$ be a smooth projective curve defined over $\mathbb{F}_q$ of genus g. Then the following hold:*

(1) (Rationality) *We have $Z(X/\mathbb{F}_q, T) \in \mathbb{Q}(T)$. More precisely, the zeta function has the form*

$$Z(X/\mathbb{F}_q, T) = \frac{\prod_{i=1}^{2g}(1-\omega_i T)}{(1-T)(1-qT)}$$

for some algebraic numbers $\omega_1, \dots, \omega_{2g}$.

(2) (Functional equation) *We have*

$$Z\left(X/\mathbb{F}_q, \frac{1}{qT}\right) = q^{1-g}\, T^{2-2g}\, Z(X/\mathbb{F}_q, T).$$

(3) (Riemann hypothesis) *The zeros of $Z(X/\mathbb{F}_q,T)$ are of absolute value $1/\sqrt{q}$. Equivalently, we have*

$$|\omega_i| = q^{1/2}, \qquad i = 1,\dots,2g.$$

Remark 21.3.2 (Weil conjectures in terms of point counting)**.** Equivalent forms of assertions (1)–(3) expressed in terms of the numbers $\#X(\mathbb{F}_{q^r})$:

(1) $\#X(\mathbb{F}_{q^r}) = 1 + q^r - \sum_{i=1}^{2g} \omega_i^r$ for some $\omega_1,\dots,\omega_{2g} \in \overline{\mathbb{Q}}$;

(2) the ω_i come in pairs $(\omega, q/\omega)$;

(3) $|\#X(\mathbb{F}_{q^r}) - 1 - q^r| = |\sum_{i=1}^{2g} \omega_i^r| \le 2g\sqrt{q}$ ("Hasse–Weil bound"), or $|\omega_i| = q^{1/2}$.

We note that (1) and (2) imply that the numbers $\#X(\mathbb{F}_{q^r})$ for $r \ge g$ determine the entire sequence (see Exercise 21.3.3 below). For example, the zeta function of an elliptic curve E over $\mathbb{F}_p$ is determined by the single number $a_p = p + 1 - \#E(\mathbb{F}_p)$.

Exercise 21.3.3. Let $\lambda_1,\dots,\lambda_g$ be complex numbers. Prove that the g numbers

$$\sum_{i=1}^{g} (\lambda_i^r + \lambda_i^{-r}), \qquad r = 1,\dots,g$$

determine the numbers $\lambda_i,\dots,\lambda_g$ up to permutation. Deduce (setting $\lambda_i = q^{-1/2}\omega_i$) that the numbers $\#X(\mathbb{F}_{q^r})$ for $r \le g$ determine the zeta function $Z(X/\mathbb{F}_q,T)$.

Remark 21.3.4 (General Weil conjectures)**.** Weil famously formulated his conjectures, the analog of Theorem 21.3.1 for an arbitrary smooth projective variety X defined over $\mathbb{F}_q$:

(1) We have

$$Z(X/\mathbb{F}_q,T) = \frac{P_1(T)P_3(T)\dots P_{2d-1}(T)}{P_0(T)P_2(T)\dots P_{2d}(T)}, \qquad d = \dim(X)$$

where $P_0(T),\dots,P_{2d}(T) \in \mathbb{Z}[T]$ are polynomials of the form

$$P_i(T) = \prod_{j=1}^{b_i} (1 - \omega_{ij}T),$$

where $P_0(T) = 1 - T$ and $P_{2d}(T) = 1 - q^dT$.

(2) We have

$$Z\left(X/\mathbb{F}_q, \frac{1}{q^dT}\right) = \pm q^{dE/2}T^E Z(X/\mathbb{F}_q,T)$$

where $E = \sum_{i=0}^{2d}(-1)^i b_i$ (the "degree" of the rational function $Z(X/\mathbb{F}_q,T)$).

(3) We have

$$|\omega_{ij}| = q^{i/2}$$

(which uniquely determines the factorization in (1)). Thus, by (2), if ω is a root of P_i, then q^d/ω is a root of P_{2d-i}.

Further, Weil conjectured a link with algebraic topology.

(4) Suppose that there exist homogeneous polynomials $f_1, \dots, f_r \in \mathbb{Z}_{(p)}[T_0, \dots, T_n]$ such that the ring $\mathbb{Z}_{(p)}[T_0, \dots, T_n]/(f_1, \dots, f_r)$ has no p-torsion and such that the projective variety defined by these equations over $\overline{\mathbb{F}}_p$ is smooth. Let $Y \subseteq \mathbb{C}P^n$ be the complex projective variety over $\mathbb{C}$ defined by the same equations (which then will be smooth as well), equipped with the analytic topology. Then the degree $b_i = \deg P_i$ is equal the dimension of the i-th singular cohomology group $H^i(Y, \mathbb{Q})$. In particular, the integer E in (2) is equal to the Euler characteristic of Y.

These conjectures have been established by Dwork (rationality), Artin–Grothendieck (rationality, functional equation, and (4)), and Deligne (who established the Riemann hypothesis in 1973). In fact, Artin and Grothendieck developed ℓ-adic cohomology $H^i(X, \mathbb{Q}_\ell)$ of any algebraic variety and recast the conjectures in terms of eigenvalues of the Frobenius map on these cohomology groups. In this formalism, assertion (1) follows from the analog of the Lefschetz fixed point formula and (2) from Poincaré duality. Assertion (4) follows from a comparison theorem between $H^i(X, \mathbb{Q}_\ell)$ and the singular cohomology $H^i(Y, \mathbb{Q}) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$. See [Hartshorne, Appendix C] for more details.

Remark 21.3.5 (Zeta functions of schemes over $\mathbb{Z}$)**.** Let X be a scheme of finite type over $\mathbb{Z}$ (for example, defined by a system of homogeneous equations with coefficients in $\mathbb{Z}[T_0, \dots, T_n]$). Let X_{cl} be its set of closed points (which correspond to maximal homogeneous ideals). As we have proved in the commutative algebra course, for every $x \in X_{\mathrm{cl}}$, the residue field $\kappa(x) = \mathcal{O}_{X,x}/\mathfrak{m}_x$ is a finite field[2]. We define the holomorphic function

$$\zeta_X(s) = \prod_{x \in X} \frac{1}{1 - \#\kappa(x)^{-s}}$$

(this converges for $\mathrm{Re}(s) > \dim(X)$). This construction has two important special cases:

(a) If $X = \mathrm{Spec}(\mathbb{Z})$, then X_{cl} is the set of prime numbers, and $\zeta_X(s) = \zeta(s)$ is the Riemann zeta function. More generally, for the ring of integers $\mathcal{O}_K$ in a number field K, the zeta function of $\mathrm{Spec}(\mathcal{O}_K)$ is the Dedekind zeta function

$$\zeta_K(s) = \prod_{0 \neq \mathfrak{p} \subseteq \mathcal{O}_K} \frac{1}{1 - \#\kappa(\mathfrak{p})^{-s}} = \sum_{0 \neq I \subseteq \mathcal{O}_K} \#(\mathcal{O}_K/I)^{-s}.$$

(b) If $X \subseteq \mathbb{P}^n$ (over $\overline{\mathbb{F}}_q$) is a projective variety defined over $\mathbb{F}_q$, and $X_0 \subseteq \mathbb{P}^n_{\mathbb{F}_q}$ is the corresponding scheme over $\mathbb{F}_q$, then

$$\zeta_{X_0}(s) = Z(X/\mathbb{F}_q, q^{-s}).$$

To see why this is true, we need a new formula for $Z(X/\mathbb{F}_q, T)$ — see Lemma 21.4.4.

In general, we do not know whether $\zeta_X(s)$ admits a meromorphic continuation to the complex plane (this would follow from the Langlands program).

21.4. The Frobenius map

The base observation is that the field $\mathbb{F}_q$ is the fixed-point set of the map $x \mapsto x^q$. We can use this to get some geometric understanding of $X(\mathbb{F}_q)$. The (q-th power) **Frobenius map** is the map

$$F\colon \mathbb{P}^n \longrightarrow \mathbb{P}^n, \qquad F(x_0 : \cdots : x_n) = (x_0^q : \cdots : x_n^q).$$

Following a familiar notation from dynamical systems, for an endomorphism $F\colon X \to X$ of a set X we denote by $\mathrm{Fix}(F) = \{x \in X : F(x) = x\}$ the set of its fixed points.

[2]**Lemma.** *If k is a field which is of finite type over $\mathbb{Z}$, then k is finite. Proof.* By Chevalley's theorem (Lecture 4, Theorem 4.4.3), the image of $\mathrm{Spec}(k) \to \mathrm{Spec}(\mathbb{Z})$ is constructible, and hence a closed point (p). Thus k is finitely generated over $\mathbb{F}_p$, and hence finite over it by Nullstellensatz (Lecture 1, Theorem 1.1.3). □

Lemma 21.4.1. *Let $X \subseteq \mathbb{P}^n$ be a locally closed subset defined over $\mathbb{F}_q$.*

(a) We have $F(X) \subseteq X$, and so F defines a map $F_X : X \to X$.

(b) $X(\mathbb{F}_{q^r}) = \mathrm{Fix}(F_X^r)$.

Proof. (a) Let $f \in \mathbb{F}_q[T_0, \ldots, T_n]$ be a homogeneous polynomial. Then

$$f(T_0^q, \ldots, T_n^q) = f(T_0, \ldots, T_n)^q,$$

and it follows that f vanishes at a point $x \in \mathbb{P}^n$ if and only if it vanishes at $F(x)$. The assertion follows since our X is defined by vanishing and non-vanishing of a system of such polynomials f.

(b) It suffices to treat the case $X = \mathbb{P}^n$ and $r = 1$. We must show that if $0 \neq (x_0, \ldots, x_n) \in \overline{\mathbb{F}}_q^{n+1}$ are such that

$$(x_0^q, \ldots, x_n^q) = \lambda \cdot (x_0, \ldots, x_n)$$

for some $\lambda \in {}^{\times}_{q}$, then there exist $(y_0, \ldots, y_n) \in \mathbb{F}_q$ and $\mu \in \overline{\mathbb{F}}_q$ such that

$$(x_0, \ldots, x_n) = \mu \cdot (y_0, \ldots, y_n).$$

To this end we set $\mu = \lambda^{1/(q-1)}$, which exists since $\overline{\mathbb{F}}_q$ is algebraically closed. □

Warning: the map $F_X : X \to X$ is bijective but not an automorphism (the extension of function fields is purely inseparable).

Definition 21.4.2. Let $X \subseteq \mathbb{P}^n$ be a locally closed subset defined over $\mathbb{F}_q$.

(a) For $x \in X$, we set $\deg(x) = \min\{r : F^r(x) = x\} =$ (the smallest r such that x is $\mathbb{F}_{q^r}$-rational).

(b) We set $X_0 = X/F_X$ to be the orbit space of the bijection F_X. Thus $\deg(x)$ is the size of the orbit of x.

Remark 21.4.3. Let $X_{00} \subseteq \mathbb{P}^n_{\mathbb{F}_q}$ be the "corresponding scheme over $\mathbb{F}_q$" as in Remark 21.3.5 (if X is closed, then X_{00} cut out by the homogeneous ideal $\mathfrak{I}(X) \cap \mathbb{F}_q[T_0, \ldots, T_n]$). Then the set $X_0 = X/F_X$ in Definition 21.4.2 coincides with the set of closed points of the scheme X_{00}, and the degree $\deg(x)$ defined above coincides with the degree of the extension $[\kappa(x) : \mathbb{F}_q]$.

Lemma 21.4.4 (Euler product)**.** *Let $X \subseteq \mathbb{P}^n$ be a locally closed subset defined over $\mathbb{F}_q$. We have*

$$Z(X/\mathbb{F}_q, T) = \prod_{x \in X_0} \frac{1}{1 - T^{\deg(x)}}.$$

Proof. Let $x \in X$, then $x \in \mathrm{Fix}(F^r) = X(\mathbb{F}_{q^r})$ if and only if the order of the orbit $\deg(x)$ divides r. Counting the fixed points in two ways, we obtain

$$\#X(\mathbb{F}_{q^r}) = \sum_{x \in X_0,\, \deg(x) | r} \deg(x).$$

Using the formula (21.2.1) we obtain

$$\begin{aligned} Z(X/\mathbb{F}_q, T) &= \exp\left(\sum_{r \geq 1} \frac{1}{r} \left(\sum_{x \in X_0,\, \deg(x) | r} \deg(x) \right) T^r \right) \\ &= \exp\left(\sum_{x \in X_0} \sum_{r :\, \deg(x) | r} \frac{\deg(x)}{r} T^r \right) = \exp\left(\sum_{x \in X_0} \sum_{r \geq 1} \frac{1}{r} T^{r \deg(x)} \right) \\ &= \prod_{x \in X_0} \exp(\log(1 - T^{\deg(x)})) = \prod_{x \in X_0} \frac{1}{1 - T^{\deg(x)}}, \end{aligned}$$

where in the third equality we substituted $r/\deg(x)$ for r. □

Suppose now that X is a smooth curve. A divisor $D = \sum a_P P$ on X is **defined over** $\mathbb{F}_q$ if $F(D) = D$, or equivalently if $a_P = a_{F(P)}$ for all $P \in X$. We denote by $\mathrm{Pic}(X_0)$ the quotient of the group of divisors defined over $\mathbb{F}_q$ by the principal divisors. We define $\mathrm{Pic}^0(X_0)$ to be the subgroup consisting of divisor classes of degree zero. It is a finite group[3] (as will follow from the computations below), and we denote its order by h (in honor of the class number). Note that if we identify $P \in X_0$ with the sum of its orbit $P + F(P) + \cdots + F^{\deg(P)-1}(P)$ then the degree of the resulting divisor equals the $\deg(x)$.

Lemma 21.4.5. *Let $X \subseteq \mathbb{P}^n$ be a smooth projective curve defined over $\mathbb{F}_q$.*

(a) We have

$$Z(X/\mathbb{F}_q, T) = \sum_{D \geq 0 \text{ def. over } \mathbb{F}_q} T^{\deg(D)}.$$

(b) For a divisor D defined over $\mathbb{F}_q$, the number of effective divisors defined over $\mathbb{F}_q$ which are linearly equivalent to D equals

$$\frac{q^{\ell(D)} - 1}{q - 1}, \qquad \ell(D) = \dim H^0(X, \mathcal{O}_X(D)).$$

(c) The degree map $\mathrm{Pic}(X_0) \to \mathbb{Z}$ is surjective.

Proof sketch. (a) Expand the Euler product in Lemma 21.4.4.

(b) These divisors are parametrized by the $\mathbb{F}_q$-rational points of the projective space $\mathbb{P}H^0(X, \mathcal{O}_X(D)) \simeq \mathbb{P}^{\ell(D)-1}$, which has

$$1 + q + \cdots + q^{\ell(D)-1} = \frac{q^{\ell(D)} - 1}{q - 1}$$

rational points.

(c) Omitted, see [Lorenzini, VIII 6.2]. The proof of this fact uses the zeta function (the fact that it has a simple pole at $T = 1$). Note that this is false over $\mathbb{R}$, for example on a real conic $C \subseteq \mathbb{P}^2$ with no rational points, every divisor defined over $\mathbb{R}$ has even degree. Finally, note that the assertion trivially holds if $X(\mathbb{F}_q)$ is non-empty, so in particular it holds after replacing $\mathbb{F}_q$ with $\mathbb{F}_{q^r}$ for some $r \geq 1$. □

21.5. Proof of Theorem 21.3.1(1): Rationality

Recall that the **Riemann–Roch theorem** on a smooth projective curve X of genus g is the formula

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

valid for every divisor D on X, where K is the canonical divisor (that is, $\mathcal{O}_X(K) \simeq \omega_X$). We can pick a K which is defined over $\mathbb{F}_q$. We have $\ell(K) = g$ and $\deg(K) = 2g - 2$. The basic corollary of Riemann–Roch is that

$$\ell(D) = \deg(D) + 1 - g \qquad \text{if } \deg(D) > 2g - 2, \tag{21.5.1}$$

as then $\deg(K - D)$ is negative and so $\ell(K - D) = 0$.

[3] **Lemma.** $\mathrm{Pic}^0(X_0)$ is finite. *Proof.* Let P be an effective divisor of degree $d > 2g - 2$ defined over $\mathbb{F}_q$. Then for every divisor D on X defined over $\mathbb{F}_q$, the divisor $D + P$ is of degree d and hence $\ell(D + P) > 0$ by Riemann–Roch. Thus $D + P \sim Q$ for an effective divisor Q defined over $\mathbb{F}_q$. Rewriting this as $D \sim Q - P$, we found a surjection from the (finite) set of all effective divisors Q of degree d defined over $\mathbb{F}_q$ onto $\mathrm{Pic}^0(X_0)$. □

Proof of Theorem 21.3.1(1). We can now prove assertion (1) of Theorem 21.3.1 by applying the formula in Lemma 21.4.5(a) and using (21.5.1). All the sums below are over divisors or divisor classes defined over $\mathbb{F}_q$.

$$\begin{aligned}
Z(X/\mathbb{F}_q,T) &= \sum_{D\geq 0} T^{\deg(D)} = \sum_{d\geq 0} \#\{D\geq 0 : \deg(D)=d\}T^d \\
&= \underbrace{\sum_{0\leq d\leq 2g-2} \#\{D\geq 0 : \deg(D)=d\}T^d}_{\text{polynomial } Q(T) \text{ of degree} \leq 2g-2} + \sum_{d>2g-2} \#\{D\geq 0 : \deg(D)=d\}T^d \\
&= Q(T) + \sum_{d>2g-2} \sum_{\mathrm{Pic}^d(X_0)} \frac{q^{\ell(D)}-1}{q-1} \\
&= Q(T) + \sum_{d>2g-2} h\cdot \frac{q^{d+1-g}-1}{q-1} T^d \\
&= \frac{P(T)}{(1-T)(1-qT)}
\end{aligned}$$

where $P(T)\in\mathbb{Z}[T]$ is a polynomial of degree $\leq 2g$ with $P(0)=1$. (In the third line, we divided the divisors of degree $d>2g-2$ into linear equivalence classes. Since they are permuted by $\mathrm{Pic}^0(X_0)$, there is h of them, and each class contributes the same number $(q^{d+1-g}-1)/(q-1)$ by (21.5.1), which gets us to the fourth line.) We shall prove that $\deg(P)=2g$ in the next step. □

21.6. Proof of Theorem 21.3.1(2): Functional equation

Proof of Theorem 21.3.1(2). The basic idea is to pair up the terms with D and $K-D$ exploiting the symmetry in the Riemann–Roch formula (Serre duality). We cannot check the formula by a simple substitution in formal power series since one side of the formula lives in $\mathbb{Q}((T))$ and the other in $\mathbb{Q}((1/T))$. So we need to be careful, and first we will treat the range of degrees from 0 to $2g-2$ separately. The key calculation is the following. Let

$$\alpha(T) = \sum_{0\leq \deg(D)\leq 2g-2} q^{\ell(D)} T^{\deg(D)}.$$

Then

$$T^{2g-2}q^{g-1}\alpha(\frac{1}{qT}) = \sum q^{\overbrace{\ell(D)-\deg(D)+g-1}^{\ell(K-D)}} T^{\overbrace{2g-2-\deg(D)}^{\deg(K-D)}} = \alpha(T).$$

Now, we can define $\beta(T)$ by

$$Z(X/\mathbb{F}_q,T) = \frac{1}{q-1}\alpha(T) + \frac{1}{q-1}\beta(T),$$

so that $Z(X/\mathbb{F}_q,T)$ satisfies the functional equation if and only if $\beta(T)$ does. Now,

$$\begin{aligned}
\beta(T) &= \sum_{\deg(D)\geq 2g-1} q^{\ell(D)}T^{\deg(D)} - \sum_{\deg(D)\geq 0} T^{\deg(D)} \\
&= \sum_{\deg(D)\geq 2g-1} q^{\deg(D)+1-g}T^{\deg(D)} - \sum_{\deg(D)\geq 0} T^{\deg(D)} \\
&= h\sum_{d\geq 2g-1} q^{d+1-g}T^d - h\sum_{d\geq 0} T^d \\
&= hq^{1-g}T^{2g-1}\frac{1}{1-qT} - h\frac{1}{1-T}.
\end{aligned}$$

We check easily that the operation $\phi \mapsto q^{1-g}T^{2g-2}\phi(q^{-1}T^{-1})$ interchanges the two summands above. □

Note that since $Z(X/\mathbb{F}_q,0)=1$, the functional equation indeed implies that the numerator $P(T)$ has degree exactly $2g$ (and leading term q^g).

21.7. Proof of Theorem 21.3.1(3): The Riemann hypothesis

Lemma 21.7.1. *Let $\lambda_1,\dots,\lambda_m$ be complex numbers and let $\rho>0$. The following conditions are equivalent*

(a) $|\lambda_i|\le\rho$ *for* $i=1,\dots,m$;

(b) $|\sum_{i=1}^m \lambda_i^r|\le m\rho^r$ *for every* $r\ge 1$.

Proof. Omitted. □

Corollary 21.7.2. *The Riemann hypothesis (3) holds if and only if the Hasse–Weil bound*

$$|\#X(\mathbb{F}_{q^r})-1-q^r|\le 2gq^{r/2}$$

is satisfied for all $r\ge 1$.

Proof. Using the formula (21.2.1), we have

$$Z(X/\mathbb{F}_q,T)=\frac{\prod_{i=1}^{2g}(1-\omega_i T)}{(1-T)(1-qT)}=\exp\left(\sum\frac{1}{r}(1+q^r-\sum_{i=1}^{2g}\omega_i^r)T^r\right),$$

from which we infer that

$$\#X(\mathbb{F}_{q^r})=1+q^r-\sum_{i=1}^{2g}\omega_i^r,$$

and consequently the left-hand side of the Hasse–Weil bound equals $|\sum\omega_i^r|$. Applying Lemma 21.7.1 with $\rho=q$ and the numbers $\omega_1,\dots,\omega_{2g}$ we see that the Hasse–Weil bound holds if and only if $|\omega_i|\le q^{1/2}$. But, by the functional equation the set $\{\omega_1,\dots,\omega_{2g}\}$ is closed under $\omega\mapsto q/\omega$. Consequently, if $|\omega_i|\le q^{1/2}$ for all i if and only if $|\omega_i|=q^{1/2}$ for all i. □

To finish the proof of (3), it suffices (changing the base field) to show the Hasse–Weil bound for $r=1$. The basic idea for this that the fixed-point set $\mathrm{Fix}(F)$ of a map $F\colon X\to X$ is the intersection of the graph Γ of F with the diagonal $\Delta\subseteq X\times X$. Since our X is a curve, the product $X\times X$ is a surface, and the number of the intersection points $\#X(\mathbb{F}_q)=\#\mathrm{Fix}(F)=\#(\Gamma\cap\Delta)$ equals the intersection number $(\Gamma.\Delta)$ which we may control using intersection theory on surfaces, notably the Hodge index theorem (Lecture 20, Theorem 20.3.1).

Lemma 21.7.3. *The curves Γ (graph of Frobenius) and Δ (diagonal) on $X\times X$ intersect transversely. Consequently,*

$$(\Gamma.\Delta)=\#X(\mathbb{F}_q).$$

Proof. Since both curves are smooth (they are isomorphic to X via the first projection $X\times X\to X$) it suffices to show that for every $(x,x)\in\Gamma\cap\Delta$, the tangent lines $T_{(x,x)}\Gamma$ and $T_{(x,x)}\Delta$ are distinct. Both are subspaces of the tangent space $T_{(x,x)}X\times X=T_xX\oplus T_xX$. The second one $T_{(x,x)}\Delta$ is simply the diagonal T_xX. We claim that $T_{(x,x)}\Gamma=T_xX\oplus 0$, which follows from the fact that since the Frobenius map is purely inseparable, its derivative vanishes everywhere. Since we have not discussed inseparable morphisms, we

do a local computation on $\mathbb{P}^n$. In an affine open $U \simeq \mathbb{A}^n \subseteq \mathbb{P}^n$ containing x, the map $\mathrm{id} \times F \colon U \to U \times U$ is given by

$$(x_1, \ldots, x_n) \mapsto (x_1, \ldots, x_n, x_1^q, \ldots, x_n^q) = (x_1, \ldots, x_n, y_1, \ldots, y_n).$$

Its image (the graph of F_U) is therefore cut out by the equations $y_i - x_i^q = 0$. Now, $dx_i^q = q x_i^{q-1} dx_i = 0$. Therefore the cotangent space is spanned by $dy_1, \ldots, dy_n$, and hence the tangent space is $U \oplus 0$. The tangent space to the graph Γ of F_x is thus contained in $T_x\mathbb{P}^n \oplus 0$, and hence equal to $T_x X \oplus 0$. □

Lemma 21.7.4. *Let $x_0 \in X$ Let $C_v = \{x_0\} \times X$ and $C_h = X \times \{x_0\}$ be the "horizontal" and "vertical" axes through $(x_0, x_0) \in X \times X$. Then*

$$a) \quad (\Delta.\Delta) = 2 - 2g, \qquad b) \quad (\Gamma.\Gamma) = q(2-2g), \qquad c) \quad (\Gamma.\Delta) = \#X(\mathbb{F}_q),$$

$$d) \quad (\Delta.C_v) = (\Delta.C_h) = (\Gamma.C_v) = 1, \qquad e) \quad (\Gamma.C_h) = q.$$

Proof. a) Follows from the adjunction formula (Lecture 19, Example 19.4.5). To show b), notice that $\Gamma = (F \times \mathrm{id})^*(\Delta)$ and $F \times \mathrm{id}$ is a finite flat morphism of degree q, so that the assertion follows from Lecture 19, Example 19.4.6. Assertion c) is the previous lemma. Formulas in d) are obvious (the intersections have only one point at which the tangent lines are distinct). Formula e) follows from the fact that $(\Gamma.C_h) = \deg(F^*(\{x_0\}) = q$. □

We proved the following result last time, as a corollary of the Hodge index theorem.

Proposition 21.7.5 (Lecture 20, Proposition 20.3.7)**.** *For any divisors D_1 and D_2 on $X \times X$ we have*

$$\begin{aligned}|(C_h \cdot D_1)(C_v \cdot D_2) + (C_h \cdot D_2)(C_v \cdot D_1) - (D_1 \cdot D_2)| \leq & \sqrt{2(C_h \cdot D_1)(C_v \cdot D_1) - (D_1 \cdot D_1)} \\ & \cdot \sqrt{2(C_h \cdot D_2)(C_v \cdot D_2) - (D_2 \cdot D_2)}.\end{aligned}$$

Proof. We work in the space $\mathrm{NS}(X)_{\mathbb{R}}$ of numerical equivalence class of divisors with real coefficients. Consider the quadratic form

$$\lambda(D) = 2(C_h.D)(C_v.D) - (D.D)$$

and the corresponding symmetric bilinear form

$$\lambda(D_1, D_2) = \frac{\lambda(D_1 + D_2) - \lambda(D_1) - \lambda(D_2)}{2} = (C_h.D_1)(C_v.D_2) + (C_h.D_2)(C_v.D_1) - (D_1.D_2).$$

Then the inequality reads

$$|\lambda(D_1, D_2)| \leq \sqrt{\lambda(D_1)\lambda(D_2)}.$$

This looks like the Cauchy–Schwarz inequality, and will follow if we show that $\lambda(D) \geq 0$ for all D.

Consider the subspace of $\mathrm{NS}(X)_{\mathbb{R}}$ spanned by the vectors $D_1 = C_h$, $D_2 = C_v$, and $D_3 = D$. Consider the determinant

$$\det[(D_i \cdot D_j)] = \begin{vmatrix} 0 & 1 & (C_h \cdot D) \\ 1 & 0 & (C_v \cdot D) \\ (C_h \cdot D) & (C_v \cdot D) & (D \cdot D) \end{vmatrix} = \lambda(D)$$

This is either zero (if D_1, D_2, and D_3 give linearly dependent elements of $\mathrm{NS}(X)_{\mathbb{R}}$), or positive otherwise (indeed, then the span of the D_i is a three-dimensional vector space on which the intersection form has signature $(1,2)$ since $(D_1 + D_2)^2 = 2 > 0$). □

Proof of Theorem 21.3.1(3). We apply Proposition 21.7.5 to $D_1 = \Gamma$ and $D_2 = \Delta$. Lo and behold:

$$\left| \underbrace{(C_h.\Delta)}_{q} \underbrace{(C_v.\Gamma)}_{1} + \underbrace{(C_h.\Gamma)}_{1} \underbrace{(C_v.\Delta)}_{1} - \underbrace{(\Delta.\Gamma)}_{\#X(\mathbb{F}_q)} \right| \leq \sqrt{2 \underbrace{(C_h.\Gamma)}_{q} \underbrace{(C_v.\Gamma)}_{1} - \underbrace{(\Gamma.\Gamma)}_{q(2-2g)}} \times \sqrt{2 \underbrace{(C_h.\Delta)}_{1} \underbrace{(C_v.\Delta)}_{1} - \underbrace{(\Delta.\Delta)}_{2-2g}} = 2g\sqrt{q}.$$

□

References

[Har77] Robin Hartshorne, *Algebraic geometry*, Graduate Texts in Mathematics, No. 52, Springer-Verlag, New York-Heidelberg, 1977. MR 463157

[IR90] Kenneth Ireland and Michael Rosen, *A classical introduction to modern number theory*, second ed., Graduate Texts in Mathematics, vol. 84, Springer-Verlag, New York, 1990. MR 1070716

[Kem93] George R. Kempf, *Algebraic varieties*, London Mathematical Society Lecture Note Series, vol. 172, Cambridge University Press, Cambridge, 1993. MR 1252397

[Lor96] Dino Lorenzini, *An invitation to arithmetic geometry*, Graduate Studies in Mathematics, vol. 9, American Mathematical Society, Providence, RI, 1996. MR 1376367

[Mum99] David Mumford, *The red book of varieties and schemes*, expanded ed., Lecture Notes in Mathematics, vol. 1358, Springer-Verlag, Berlin, 1999, Includes the Michigan lectures (1974) on curves and their Jacobians, With contributions by Enrico Arbarello. MR 1748380