1. Week One

Let k be a finite field, and let q denote the number of elements in k. One of the main objectives of this course is to study systems of polynomial equations over k. That is, let

$$f_j(x_1, \ldots, x_n) \in k[x_1, \ldots, x_n] , \qquad 1 \leq j \leq r$$

be polynomials, and consider the system

$$f_j(x_1, \ldots, x_n) = 0 , \qquad \text{for all } 1 \leq j \leq r .$$

A typical problem is to estimate the number N of solutions to this system in k^n. Obviously one has the trivial estimate $0 \leq N \leq q^n$, but we hope to do better.

Another point of view is to consider a system of polynomial equations

$$F_j(x_1, \ldots, x_n) = 0 , \qquad \text{for all } 1 \leq j \leq r ,$$

where $F_j \in \mathbb{Z}[x_1, \ldots, x_n]$, $1 \leq j \leq r$ are polynomials with *integer* coefficients. One approach to these so-called Diophantine equations is to reduce them to a system of congruences

$$F_j(x_1, \ldots, x_n) \equiv 0 \pmod{p} , \text{ for all } 1 \leq j \leq r,$$

where p is a prime number. Clearly this is equivalent to studying the solutions to equations over the finite field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

Example 1.1. Fix an integer $n \geq 1$, and let N_p denote the number of solutions in $\mathbb{F}_q^2$ to the equation $x^n + y^n = 1$. One can show that $|N_p - p| \leq Cp^{1/2}$, for a constant C not depending on p. More generally, if X is the irreducible variety defined by the system $f_j(x_1, \ldots, x_n) = 0$, for all $1 \leq j \leq r$, then a theorem of Lang and Weil asserts that

$$|N_p - p^{\dim(X)}| \leq Cp^{\dim(X)-1/2} .$$

Notice that this estimate gets better as p gets larger. But for small p, depending on the constant C, this estimate might be terrible, even worse than $0 \leq N_p \leq p^n$! This is unfortunate, because in applications (coding theory, cryptography, finite geometry, combinatorics, etc.) one may want good bounds for small p, in which case the Lang-Weil estimate is of no use.

1.1. Basic Facts About Finite Fields.

As before, let k be a finite field with q elements. Since $1 \in k$ we have the obvious map $\mathbb{Z} \to k$ $(n \mapsto n \cdot 1)$. This map can't be injective, since k is finite, and therefore its kernel is $p\mathbb{Z}$ for some prime number p. (We know the kernel is prime because k has no zero-divisors.) We call p the *characteristic* of k. So we have an inclusion $\mathbb{Z}/p\mathbb{Z} \hookrightarrow k$, which makes k into a $\mathbb{Z}/p\mathbb{Z}$-vector space. Thus it has a dimension, say m, where $1 \leq m < \infty$. We conclude that $q = p^m$, and as $\mathbb{Z}/p\mathbb{Z}$-vector spaces (and in particular as additive groups) we have $k \simeq (\mathbb{Z}/p\mathbb{Z})^m$.

Theorem 1.2. *For every prime p and integer $m \geq 1$, there exists a finite field with p^m elements. Moreover, any two such fields are isomorphic. (We therefore denote by $\mathbb{F}_q$ the unique finite field with q elements.)*

Proof. Let F be an algebraic closure of the field $\mathbb{Z}/p\mathbb{Z}$. Then clearly all finite fields of characteristic p are contained in F, since they are finite, and therefore algebraic, extensions of $\mathbb{Z}/p\mathbb{Z}$. Suppose we have $k \subseteq F$, where $\#k = q$. Then $\#k^* = q-1$, and so by Lagrange's theorem we have $\alpha^{q-1} = 1$ for all $\alpha \in k^*$. Thus $\alpha^q = \alpha$ for all $\alpha \in k$. This argument shows that every element of k is a root of the polynomial $f(x) = x^q - x$. Since there are at most q roots to this polynomial, k must represent all of its roots. In other words, we have

$$k = \{\alpha \in F \mid \alpha^q = \alpha\} \ .$$

Since the right hand side of this equality depends only on the prime p and the number q, this shows uniqueness (up to isomorphism.)

To show existence, we only need to show that given a prime power $q = p^m$, the set $k = \{\alpha \in F \mid \alpha^q = \alpha\}$ is a field with q elements. Since k is the set of roots in F of the polynomial $f(x) = x^q - x$, we know that $\#k \leq q$. On the other hand, $f'(x) = qx^{q-1} - 1 = -1 \neq 0$ in F. Therefore f has distinct roots, forcing $\#k = q$. To show that k is a field, we first observe that $0, 1 \in k$. If $a, b \in k$, then we have $(ab)^q = a^q b^q = ab$, and $(a^{-1})^q = (a^q)^{-1} = a^{-1}$. Also,

$$(-a)^q = (-1)^q a^q = (-1)^q a = \begin{cases} -a & \text{if } q \text{ is odd} \\ a & \text{if } q \text{ is even} \end{cases} = -a \ .$$

Finally, we need to show that $(a+b)^q = a^q + b^q = a + b$, which follows from the following.

Lemma 1.3. *If K is field of characteristic p, then for any $m \geq 1$ and any $x, y \in K$,*

$$(x+y)^{p^m} = x^{p^m} + y^{p^m} \ .$$

Proof. We have

$$(x+y)^p = \sum_{i=0}^{p} \binom{p}{i} x^i y^{p-i} = x^p + y^p \ ,$$

since $p | \binom{p}{i}$ whenever $1 \leq i \leq p-1$. We proceed by induction on m. Assume the truth of the lemma for exponent $m-1$, and we have

$$\begin{aligned} (x+y)^{p^m} &= ((x+y)^p)^{p^{m-1}} = (x^p + y^p)^{p^{m-1}} \\ &= (x^p)^{p^{m-1}} + (y^p)^{p^{m-1}} = x^{p^m} + y^{p^m} \end{aligned}$$

by the induction hypothesis. □

The theorem follows immediately from this lemma. □

1.2. **Constructing Finite Fields.** The proof of the above theorem is slick, but it doesn't really lend itself to actually getting one's hands on the field $\mathbb{F}_q$ and computing in it. The most concrete way to represent the field $\mathbb{F}_q$, where $q = p^m$, is to find an irreducible polynomial $g(x) \in \mathbb{F}_p$ of degree m. In that case, it is plain to see by uniqueness that we must have

$$\mathbb{F}_q \simeq \mathbb{F}_p[x]/(g(x)) \ .$$

(One has to show that the right hand side is a field. Recall that all primes are maximal in a Euclidean ring, and that $\mathbb{F}_p[x]$ is Euclidean.) For example, $x^3 + x + 1$ is irreducible over $\mathbb{F}_2$ since it's a cubic with no roots, and therefore $\mathbb{F}_8 \simeq \mathbb{F}_2[x]/(x^3 + x + 1)$.

Remarks 1.4. Suppose q is a prime power and $d \geq 1$ is in integer. Then for $\alpha \in \mathbb{F}_q$ we have $\alpha^{q^d} = \alpha^{(q \cdot q \cdot q \cdots q)} = \alpha$. Thus $\mathbb{F}_q \subseteq \mathbb{F}_{q^d}$. Conversely, if $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$, then $p^n = (p^m)^d$ for some integer d, since $\mathbb{F}_{p^n}$ is a $\mathbb{F}_{p^m}$-vector space. Therefore $m|n$. This argument shows that for any prime p, we have the rule

$$\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n} \text{ if and only if } m \mid n \ .$$

Also, since any finite field $\mathbb{F}_q$ is the splitting field of $x^q - x$, it is Galois over the prime field $\mathbb{F}_p$. Therefore *any* extension of finite fields $\mathbb{F}_{q^d}/\mathbb{F}_q$ is Galois.

By the above lemma, the map $\alpha \mapsto \alpha^q$ is an automorphism of $\mathbb{F}_{q^d}$ fixing $\mathbb{F}_q$. This element has order d in the Galois group. (To see this, let r be its order. Then $\alpha \mapsto \alpha^{q^r}$ is the identity on $\mathbb{F}_{q^d}$. Thus all q^d elements of $\mathbb{F}_{q^d}$ are roots of the polynomial $x^{q^r} - x$. This is a contradiction unless $d \leq r$. Since $r \mid [\mathbb{F}_{q^d} : \mathbb{F}_q] = d$, this shows $r = d$.) Since $d = [\mathbb{F}_{q^d} : \mathbb{F}_q]$, we have shown that $\mathrm{Gal}(\mathbb{F}_{q^d}/\mathbb{F}_q)$ is cyclic, generated by the map $\alpha \mapsto \alpha^q$.

The last basic fact about finite fields that we will need is the following theorem, which determines the structure of their multiplicative groups. The proof will make use of the classification theorem of finite abelian groups.

Theorem 1.5. *$\mathbb{F}_q^*$ is cyclic.*

Proof. We know that $\mathbb{F}_q^*$ is a finite abelian group, so it has the shape

$$\mathbb{F}_q^* \simeq (\mathbb{Z}/d_1\mathbb{Z}) \oplus (\mathbb{Z}/d_2\mathbb{Z}) \oplus \cdots \oplus (\mathbb{Z}/d_r\mathbb{Z})$$

where $d_1 \mid d_2 \mid \cdots \mid d_r$ and $d_1 > 1$. If $r > 1$, then there is a copy of $\mathbb{Z}/d_1\mathbb{Z}$ inside $\mathbb{Z}/d_2\mathbb{Z}$, since $d_1 \mid d_2$. Thus there are (at least) two cyclic subgroups of $\mathbb{F}_q^*$ of order d_1 which intersect to the identity. Therefore there are at least $2d_1 - 1$ elements of $\mathbb{F}_q^*$ which are roots of the polynomial $x^{d_1} - 1$. This is contradiction, since $d_1 < 2d_1 - 1$ and a degree d_1 polynomial can have at most d_1 roots in any field. Therefore $r = 1$. □

We have the following

Corollary 1.6. *For any $n \geq 1$,*

$$S_n = \sum_{x \in \mathbb{F}_q} x^n = \begin{cases} 0 & \text{if } (q-1) \nmid n \\ -1 & \text{if } (q-1) \mid n \ . \end{cases}$$

Proof. Notice that we can omit the zero term in the sum S_n, so that if $(q-1) \mid$ we have

$$S_n = \sum_{x \in \mathbb{F}_q^*} x^n = \sum_{x \in \mathbb{F}_q^*} 1 = q - 1 = -1 \text{ in } \mathbb{F}_q \ .$$

On the other hand, if $(q-1) \nmid n$, we let $\mathbb{F}_q^*$ have generator g. Then $g^n \neq 1$, so

$$S_n = \sum_{i=0}^{q-2} (g^i)^n = \sum_{i=0}^{q-2} (g^n)^i = \frac{(g^n)^{q-1} - 1}{g^n - 1} = \frac{1 - 1}{g^n - 1} = 0 \ .$$

□

We will use the sum S_n in the following

Lemma 1.7. *Let $f \in \mathbb{F}_q[x_1, \ldots, x_n]$, where $\mathrm{char}(\mathbb{F}_q) = p$, and let $N(f)$ denote the number of solutions to the equation $f(x_1, \ldots, x_n) = 0$ in $\mathbb{F}_q^n$. Write*

$$f(x_1, \ldots, x_n)^{q-1} = \sum a_{i_1, i_2, \ldots, i_n} x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n} \ .$$

Then the following congruence holds:

$$N(f) \equiv (-1)^{n+1} \sum_{\substack{i_1, i_2, \ldots i_n > 0 \\ (q-1) | i_1, i_2, \ldots, i_n}} a_{i_1, i_2, \ldots, i_n} \pmod{p} \ .$$

Aside 1.8. *A priori it is not even obvious that the right hand side of this congruence is an element of the prime field $\mathbb{F}_p$.*

Proof. If $(\alpha_1, \ldots, \alpha_n) \in \mathbb{F}_q^n$, then

$$1 - f(\alpha_1, \ldots, \alpha_n)^{q-1} = \begin{cases} 1 & \text{if } f(\alpha_1, \ldots, \alpha_n) = 0 \\ 0 & \text{if } f(\alpha_1, \ldots, \alpha_n) \neq 0 \ . \end{cases}$$

Thus, in a sense, $1 - f^{q-1}$ is the characteristic function of the zero set of f. Therefore

$$\begin{aligned} N(f) &\equiv \sum_{(\alpha_1, \ldots, \alpha_n) \in \mathbb{F}_q^n} \big(1 - f(\alpha_1, \ldots, \alpha_n)^{q-1}\big) \pmod{p} \\ &\equiv - \sum_{(\alpha_1, \ldots, \alpha_n) \in \mathbb{F}_q^n} f(\alpha_1, \ldots, \alpha_n)^{q-1} \pmod{p} \\ &\equiv - \sum_{(\alpha_1, \ldots, \alpha_n) \in \mathbb{F}_q^n} \sum_{i_1, \ldots, i_n} a_{i_1, i_2, \ldots, i_n} \alpha_1^{i_1} \alpha_2^{i_2} \cdots \alpha_n^{i_n} \pmod{p} \\ &\equiv - \sum_{i_1, \ldots, i_n} a_{i_1, i_2, \ldots, i_n} \Big\{ \sum_{(\alpha_1, \ldots, \alpha_n) \in \mathbb{F}_q^n} \alpha_1^{i_1} \alpha_2^{i_2} \cdots \alpha_n^{i_n} \Big\} \pmod{p} \ . \end{aligned}$$

Factoring the inner sum, we get

$$\begin{aligned} \sum_{(\alpha_1, \ldots, \alpha_n) \in \mathbb{F}_q^n} \alpha_1^{i_1} \alpha_2^{i_2} \cdots \alpha_n^{i_n} &= \prod_{j=1}^{n} \Big(\sum_{\alpha_j \in \mathbb{F}_q} \alpha_j^{i_j} \Big) \\ &= \prod_{j=1}^{n} \Big(S_{i_j} \Big) = \begin{cases} (-1)^n & \text{when } i_j > 0 \text{ and } (q-1) \mid i_j \text{ for all } j \\ 0 & \text{otherwise} \ . \end{cases} \end{aligned}$$

Plugging this in to the above calulation for $N(f)$, we are done. □

1.3. **Application I: The Hasse Invariant.** Let q a power of the odd prime p, let $a, b \in \mathbb{F}_q$, and let $f(x,y) = y^2 - x^3 - ax - b$. Then

$$(y^2 - x^3 - ax - b)^{q-1} = \sum_{j=0}^{q-1} \binom{q-1}{j} y^{2j}(-x^3 - a1x - b)^{q-1-j} \ .$$

By the lemma, the only terms of this sum that will contribute modulo p to $N(f)$ are $j = (q-1)/2$ and $j = (q-1)$. But the term $\binom{q-1}{q-1} y^{2(q-1)}(-x^3 - ax - b)^0$ has no x terms in it, so it doesn't contribute either. Observing that

$$\deg\Big((-x^3 - ax - b)^{(q-1)/2}\Big) = 3(q-1)/2 < 2(q-1) \ ,$$

we see that only the x^{q-1} term in the expansion of $(-x^3 - ax - b)^{(q-1)/2}$ will show up in the sum for $N(f)$. Letting A be the coefficient of x^{q-1} in $(-x^3 - ax - b)^{(q-1)/2}$, we conclude that

$$\begin{aligned} N(f) &\equiv (-1)^{(q-1)/2} \binom{q-1}{(q-1)/2} A \pmod{p} \\ &\equiv A \pmod{p} \ . \end{aligned}$$

This residue class A is called the *Hasse invariant* of the elliptic curve $f(x,y) = 0$, defined over $\mathbb{F}_q$.

1.4. **Application II: The Chevalley-Warning Theorem.** This result, originally conjectured by Artin, allows one to infer, modulo p, the number of solutions to certain equations. As usual, we let $\mathbb{F}_q$ be a finite field of characteristic p, $f \in \mathbb{F}_q[x_1, \ldots, x_n]$, and we denote by $N(f)$ the number of solutions in $\mathbb{F}_q^n$ of $f(x_1, \ldots, x_n) = 0$.

Theorem 1.9. *If* $\deg(f) < n$, *then* $N(f) \equiv 0 \pmod{p}$.

Proof. The idea is to show that the sum in the lemma is the empty sum, and therefore zero. Write $f(x_1, \ldots, x_n)^{q-1} = \sum a_{i_1,i_2,\ldots,i_n} x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}$, and suppose the coefficient $a_{i_1,i_2,\ldots,i_n} \neq 0$ qualifies for inclusion in the sum in the conclusion of the lemma. That is, it satisfies $i_j > 0$ and $(q-1) | i_j$ for all j. Then $i_j \geq q-1$ for all j, and therefore $i_1 + \cdots + i_n \geq n(q-1)$. Then we have

$$n(q-1) \leq i_1 + \cdots + i_n \leq \deg(x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}) \leq \deg(f^{q-1}) = (q-1)\deg f \ .$$

We conclude that $n \leq \deg f$, a contradicion of the hypothesis. Therefore the sum in the conclusion of the lemma is the empty sum. □

Remarks 1.10. An easy consequence of the Chevalley-Warning theorem is that, if $\deg f < n$ and $N(f) \geq 1$, then $N(f) \geq p$. In particular, since homogeneous polynomials always have the zero solution, the theorem will provide some non-zero solutions. For example, applying the theorem to an irreducible quadratic homogeneous polynomial in three variables, we find that all conics have rational points over a finite field (projectively).

Let $f(x,y) = x^2 + xy + y^2 \in \mathbb{F}_q[x,y]$. Since the degree is equal to the number of variables, this polynomial narrowly misses the hypothesis of the theorem. And indeed, by inspection we see $N(f) = 1 \not\equiv 0 \pmod{2}$. Actually, f factors as $f(x,y) = (x + wy)(x + w^2 y)$ where

$w \in \mathbb{F}_4$ satisfies $w^2 + w + 1 = 0$. Even though this is a trivial example, it suggests a generalization.

Given a finite field $\mathbb{F}_q$ and an integer $n \geq 2$, we will construct a polynomial $f(x_1, \ldots, x_n) \in \mathbb{F}_q[x_1, \ldots, x_n]$, of degree n, such that $N(f) = 1$. This will show that the Chevalley-Warning theorem is sharp, in the sense that the requirement $\deg f < n$ in the hypothesis cannot be weakened. Let $\alpha_1, \ldots, \alpha_n$ be a basis for $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. For each $1 \leq i \leq n$, let $\alpha_i^{(1)}, \ldots, \alpha_i^{(n)}$ be the Galois conjugates of α_i in the field extension $\mathbb{F}_{q^n}/\mathbb{F}_q$. We define

$$h_n(x_1, \ldots, x_n) = \prod_{j=1}^{n} \left(\alpha_1^{(j)} x_1 + \cdots + \alpha_n^{(j)} x_n \right) .$$

By the action of Galois, we see that h_n has coefficients in $\mathbb{F}_q$. Suppose $f(a_1, \ldots, a_n) = 0$. Then $\alpha_1^{(j)} a_1 + \cdots + \alpha_n^{(j)} a_n = 0$ for some j. But since the $\alpha_1, \ldots, \alpha_n$ are linearly independent over $\mathbb{F}_q$, so are the conjugates $\alpha_1^{(j)}, \ldots, \alpha_n^{(j)}$. Therefore $a_1 = a_2 = \cdots = a_n = 0$. So the only solution is the zero solution, whereby $N(h_n) = 1$.

2. Week two

From last time,

Theorem 2.1 (Chevalley–Warning)**.** *If $f(x_1, \ldots, x_n) \in \mathbb{F}_q[x_1, \ldots, x_n]$ for $q = p^m$ (p prime), and $\deg(f) < n$, then $\#\{(a_1, \ldots, a_n) \in \mathbb{F}_q^n \mid f(a_1, \ldots, a_n) = 0\} \equiv 0 \pmod{p}$.*

Recall that we showed that for all q and $n \geq 1$, there exist homogeneous polynomials $h_n(x_1, \ldots, x_n) \in \mathbb{F}_q[x_1, \ldots, x_n]$, with $\deg(h_n) = n$, such that the only common solution to the h_n's in $\mathbb{F}_q^n$ is $(0, \ldots, 0)$. Hence, the requirement that $\deg(f) < n$ in the result really is necessary.

Corollary 2.2. *If $f_1, \ldots, f_k \in \mathbb{F}_q[x_1, \ldots, x_n]$ with*

$$k \cdot \max_{1 \leq i \leq k} \deg(f_i) < n \ ,$$

and such that $f_i(0, \ldots, 0) = 0$ for all i, then there exists $(a_1, \ldots, a_n) \in \mathbb{F}_q \setminus \{(0, \ldots, 0)\}$ such that $f_i(a_1, \ldots, a_n) = 0$ for $i = 1, \ldots, n$.

In fact, one can replace the hypothesis that $f_i(0, \ldots, 0) = 0$ for all i to the assumption that the f_i's have *any* common zero, as it can be changed to $(0, \ldots, 0)$ by a linear change of variables. So the Corollary states that if the f_i's have one common zero in $\mathbb{F}_q^n$, then they must have another.

Proof. Let $f = h_k(f_1, \ldots, f_k)$ (for the function h_k discussed above). Observe that f is the sum of monomials of the form $c \cdot {f_1}^{i_1} \cdots {f_k}^{i_k}$, where $i_1 + \ldots + i_k = \deg h_k = k$, so the monomial has degree $= i_1 \deg f_1 + \ldots + i_k \deg f_k \leq (i_1 + \ldots + i_k) \max(\deg f_i) < n$, hence $\deg(f) < n$.

So by the Chevalley–Warning theorem, there exists $(a_1, \ldots, a_n) \in \mathbb{F}_q \setminus \{(0, \ldots, 0)\}$ such that $f(a_1, \ldots, a_n) = h_k(f_1(a_1, \ldots, a_n), \ldots, f_k(a_1, \ldots, a_n)) = 0$; the properties of h_k thus imply that $f_i(a_1, \ldots, a_n) = 0$ for all i. (Indeed, there exist at least $p - 1$ such $(a_1, \ldots, a_n)$'s.) ∎

We will next discuss systems of equations of low degree. The solution of degree 1 systems follows from linear algebra. The next case is degree 2:

2.1. **Conics.** Let $f(x,y) \in \mathbb{F}_q[x,y]$ be of degree 2. We want to know $N(f) = \#\{(a,b) \in \mathbb{F}_q^2 \mid f(a,b) = 0\}$. There are three cases to consider.

2.1.1. *Case One.* Suppose f factors over $\mathbb{F}_q$; say $f(x,y) = L_1(x,y) \cdot L_2(x,y)$, for $L_1, L_2 \in \mathbb{F}_q[x,y]$ of degree 1. Now, $f = 0$ iff $L_1 = 0$ or $L_2 = 0$, so $N(f) = 2q$ or $2q-1$, depending on whether the sets $\{L_1 = 0\}$ and $\{L_2 = 0\}$ intersect or not.

2.1.2. *Case Two.* Say $f = L_1 \cdot L_2$, with $\deg(L_i) = 1$, but L_1, L_2 *not* having coefficients in $\mathbb{F}_q$. For all $\sigma \in G = \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$, $f = f^\sigma = L_1^\sigma L_2^\sigma$. But polynomial rings are UFD's, thus $\{L_1, L_2\} = \{L_1^\sigma, L_1^\sigma\}$ (actually, the L_i^σ's may be off from L_1 or L_2 by a constant factor; this can be avoided without loss of generality by, say, scaling the L_i's to make certain coefficients equal to 1).

Hence, G acts on the set $\{L_1, L_2\}$, giving a representation $\varphi : G \to \mathrm{S}_2$. The map cannot be trivial, as otherwise we would have ${L_i}^\sigma = L_i$ for all σ, implying $L_i \in \mathbb{F}_q[x,y]$ (note that it also follows that $L_1 \neq L_2$). Hence $(\ker\varphi)$ will be of the form $\mathrm{Gal}(\overline{\mathbb{F}}_q/k)$, for some field $k \supseteq \mathbb{F}_q$ with $[G : \mathrm{Gal}(\overline{\mathbb{F}}_q/k)] = 2$, thus $[k : \mathbb{F}_q] = 2$. But the only degree 2 extension of $\mathbb{F}_q$ is $\mathbb{F}_{q^2}$, so we conclude that $L_1, L_2 \in \mathbb{F}_{q^2}[x,y]$.

Now suppose $P \in \{L_1 = 0\} \setminus \{L_2 = 0\}$, and choose a $\sigma \in G \setminus \ker(\varphi)$. Then $P^\sigma \in \{L_2 = 0\}$, so $P^\sigma \neq P$ and thus $P \notin \mathbb{F}_q^2$. Therefore $N(f) = \#(\{L_1 = 0\} \cap \{L_2 = 0\})$. However, since $L_1 \neq L_2$ (as remarked above), the lines $\{L_1 = 0\}$ and $\{L_2 = 0\}$ intersect in at most one point, and we conclude that $N(f)$=0 or 1.

Definition 2.3. A polynomial $f \in k[x_1, \ldots, x_n]$ is *irreducible* if whenever $f = g \cdot h$ (for $g, h \in k[x_1, \ldots, x_n]$) then g or $h \in k$. We say f is *absolutely irreducible* if it is irreducible in $\overline{k}[x_1, \ldots, x_n]$.

2.1.3. *Case Three.* Suppose f is absolutely irreducible. Let $F(x,y,z) = z^2 f\left(\frac{x}{z}, \frac{y}{z}\right)$, the *homogenization* of f. Why? Because now F is a polynomial of degree 2 in 3 variables, and we may apply the Chevalley–Warning Theorem. As $F(0,0,0) = 0$, there exists $(a,b,c) \in \mathbb{F}_q^3 \setminus \{(0,0,0)\}$ such that $F(a,b,c) = 0$. If $c \neq 0$, then $f\left(\frac{a}{c}, \frac{b}{c}\right) = 0$, and we have a point P on the curve $\{f = 0\}$. (If $c = 0$, then, say, $a \neq 0$, and we could instead use $F\left(1, \frac{b}{a}, \frac{c}{a}\right) = 0$ and look at $g(x,y) = F(1,x,y)$; as we will be looking at projective points in a moment anyway, this won't matter.)

Now that we have a point, we can consider lines with "rational slope" through that point and find their intersections with the curve. Without loss of generality, our point P is $(0,0)$. Now, say

$$f(x,y) = ax + by + cx^2 + dxy + ey^2.$$

It follows from absolute irreducibility that there is a unique tangent line at P, namely $ax + by = 0$, which intersects the curve only at P. If we do the linear change of variables $ax + by \to x$, $ux + vy \to y$ for some u, v such that $av - bu \neq 0$ (which will always exist), then our curve becomes

$$x + \gamma x^2 + \delta xy + \epsilon y^2 = 0,$$

and the tangent line has become $x = 0$. All non-tangent lines through P on this curve have the form $y = tx$ for some $t \in \mathbb{F}_q$, so there are q of these. Each of the rational points $\neq P$ on the curve, even the points at infinity, lies on exactly one such line, and conversely, each line intersects the curve in exactly one point besides P. Hence the total number of (projective) points is $q + 1$. Indeed, for a fixed t,

$$f(x, tx) = x + (\gamma + \delta t + \epsilon t^2)x^2,$$

so the roots are $x = 0$ (corresponding to P) and $x(t) := \frac{-1}{\gamma+\delta t+\epsilon t^2}$. The points at infinity correspond to the zeros of the denominator, hence there are 0, 1, or 2 of these. In summary, for each $t \in \mathbb{F}_q$ such that $\gamma + \delta t + \epsilon t^2 \neq 0$, we get a point $(x(t), t \cdot x(t)) \neq P$ on the curve. Hence $N(f) = q - 1$, q, or $q + 1$ (depending on the discriminant of $\gamma + \delta t + \epsilon t^2$).

Projective Spaces

Let k be a field, and n a non-negative integer. We define *n-dimensional projective space over k*, denoted $\mathbb{P}^n(k)$, as follows. Put an equivalence relation on $k^{n+1} \setminus \{(0, \ldots, 0)\}$ by saying $(a_0, \ldots, a_n) \sim (b_0, \ldots, b_n)$ if and only if there exists $\lambda \in k^*$ such that $a_i = \lambda b_i$ for all i. Then

$$\mathbb{P}^n(k) = \frac{k^{n+1} \setminus \{(0, \ldots, 0)\}}{\sim}$$

Equivalently, $\mathbb{P}^n(k)$ is the set of all lines through the origin in k^{n+1}. We represent the equivalence class containing $(a_0, \ldots, a_n)$ by $(a_0 : \ldots : a_n)$.

Remarks. We note the following:

- If we have $(a_0, \ldots, a_n)$ with $a_i = 0$, then $b_i = 0$ for any $(b_0, \ldots, b_n) \sim (a_0, \ldots, a_n)$. So we can unambiguously talk about whether or not $a_i = 0$ in $(a_0 : \ldots : a_n)$.
- Consider $U_0 = \{(a_0 : \ldots : a_n) \in \mathbb{P}^n(k) \mid a_0 \neq 0\}$. We have a well-defined map:

$$\begin{array}{ccc} U_0 & \longrightarrow & k^n \\ (a_0 : \ldots : a_n) & \longmapsto & \left(\frac{a_1}{a_0} : \ldots : \frac{a_n}{a_0}\right) \end{array}$$

  It has the inverse $(a_1, \ldots, a_n) \mapsto (1 : a_1 : \ldots : a_n)$, making it a bijection. Also, we have the map:

$$\begin{array}{ccc} \mathbb{P}^n \setminus U_0 & \longrightarrow & \mathbb{P}^{n-1} \\ (0 : a_1 : \ldots : a_n) & \longmapsto & (a_1 : \ldots : a_n) \end{array}$$

  which is also clearly a bijection. Hence, we can decompose $\mathbb{P}^n$:

$$\begin{array}{ccccc} \mathbb{P}^n(k) & = & U_0 & \cup & (\mathbb{P}^n \setminus U_0) \\ & & \updownarrow & & \updownarrow \\ & & k^n & & \mathbb{P}^{n-1} \end{array}$$

  Continuing this, we see that $\mathbb{P}^n(k) = k^n \cup k^{n-1} \cup \ldots \cup k^0$ (where $k^0 = \mathbb{P}^0(k) =$ one point); hence $\#\mathbb{P}^n(k) = q^n + q^{n-1} + \cdots + 1 = \frac{q^{n+1}-1}{q-1}$, if $k = \mathbb{F}_q$.

Consider the particular case of $\mathbb{P}^1$:

$$\begin{array}{ccccc} \mathbb{P}^1 & = & U_0 & \cup & \{\infty\} \\ & & \updownarrow & & \updownarrow \\ & & k & & \text{“point at infinity”} \end{array}$$

If we have a rational function $f(x) \in k(x)$, we may think of $f(x)$ as an honest function $f : \mathbb{P}^1 \to \mathbb{P}^1$; indeed, write $f(x) = A(x)/B(x)$, where $\gcd(A, B) = 1$ (this makes sense as $k[x]$ is a PID). Then for $\alpha \in k$,

$$f(\alpha) = \begin{cases} A(\alpha)/B(\alpha) & \text{if } B(\alpha) \neq 0, \\ \infty & \text{if } B(\alpha) = 0 \end{cases}$$

and

$$f(\infty) \quad \left(= \text{“}\lim_{x \to 0} \frac{A(1/x)}{B(1/x)}\text{”} \right) \quad = \quad \begin{cases} \infty & \text{if } \deg(A) > \deg(B) \\ 0 & \text{if } \deg(A) < \deg(B) \\ a_0/b_0 & \text{if } \deg(A) = \deg(B) \end{cases}$$

(where a_0, b_0 are the leading coefficients of A, B.)

Now consider $\mathbb{P}^2$:

$$\begin{array}{ccccc} \mathbb{P}^2 & = & U_0 & \cup & \mathbb{P}^1 \\ & & \updownarrow & & \updownarrow \\ & & k^2 & & \text{“line at infinity”} \end{array}$$

Definition 2.4. A *line* in $\mathbb{P}^2$ is a set

$$L = \{(a_0 : a_1 : a_2) \in \mathbb{P}^2(k) \mid \alpha_0 a_0 + \alpha_1 a_1 + \alpha_2 a_2 = 0\}$$

for some $\alpha_0, \alpha_1, \alpha_2 \in k$, not all $= 0$.

Note that this is well-defined. Also, note that scaling $(\alpha_0, \alpha_1, \alpha_2)$ by some element of k^* doesn't change L; hence L depends only on $(\alpha_0 : \alpha_1 : \alpha_2)$.

Consider k^2 to be embedded into $\mathbb{P}^2(k)$ as U_0. Then $L \cap k^2$ is the set $\{(x, y) \in k^2 \mid \alpha_0 + \alpha_1 x + \alpha_2 y = 0\}$, which is the usual kind of line in the plane, except when $\alpha_1 = \alpha_2 = 0$, in which case $L \cap k^2 = \emptyset$, and L is the line at infinity ($\mathbb{P}^2 \setminus U_0$).

Exercise 2.1. If $L_1 \neq L_2$ are lines in $\mathbb{P}^2$, then $L_1 \cap L_2$ is a point.

Exercise 2.2. Show that the “dual map”

$$\left\{(a_0 : a_1 : a_2) \in \mathbb{P}^2(k)\right\} \Big| \sum \alpha_i a_i = 0\} \quad \longrightarrow \quad (\alpha_0 : \alpha_1 : \alpha_2) \in \mathbb{P}^2(k)$$

is a bijection between $\mathbb{P}^2$ and the set of lines in $\mathbb{P}^2$. (Observe that under this duality, the statement in Exercise 1 corresponds to the statement that between any two points, there exists a unique line.)

Let $f(x) \in k[x_0, \ldots, x_n]$ be a homogeneous polynomial. For all $\lambda \in k$, $f(\lambda a_0, \ldots, \lambda a_n) = \lambda^{\deg f} f(a_0, \ldots, a_n)$ hence the condition $f(a_0, \ldots, a_n) = 0$ depends only on $(a_0 : \ldots : a_n) \in \mathbb{P}^n(k)$. So given homogeneous polynomials (perhaps of different degrees) $f_1, \ldots, f_m \in k[x_0, \ldots, x_n]$, it makes sense to define the set of common zeros in $\mathbb{P}^n$:

$$X = \{(a_0 : \ldots : a_n) \in \mathbb{P}^n(k) \mid f_i(a_0, \ldots, a_n) = 0 \text{ for all } i\}.$$

Definition 2.5. A *projective conic* is the set of zeros in $\mathbb{P}^2(k)$ of a homogeneous, degree 2 polynomial in $k[x_0, x_1, x_2]$.

What is the set of all lines through a given point $(a_0 : a_1 : a_2) \in \mathbb{P}^2$? Well, the set of lines $L = \{(x_0 : x_1 : x_2) \in \mathbb{P}^2 \mid \alpha_0 x_0 + \alpha_1 x_1 + \alpha_2 x_2 = 0\}$ containing $(a_0 : a_1 : a_2)$ corresponds to the set of points $(\alpha_0 : \alpha_1 : \alpha_2)$ such that $\alpha_0 a_0 + \alpha_1 a_1 + \alpha_2 a_2 = 0$, which is itself a line! That is, the set of lines through a given point of $\mathbb{P}^2$ is a line in the dual $\mathbb{P}^2$.

Remarks. Given two distinct lines L_1 and L_2 and a point P_0 belonging to *neither* line, we obtain a bijection $f : L_1 \to L_2$ by drawing lines through P_0: $f(P) = L_2 \cap \overline{P\,P_0}$, $f^{-1}(Q) = L_1 \cap \overline{Q\,P_0}$

Theorem 2.6. *Suppose X is an absolutely irreducible projective conic, and we have a point $P_0 \in X(k)$. Then $X(k)$ is in bijection with $\mathbb{P}^1(k)$ by the map (composed with the dual map):*

$$P \in X(k) \mapsto \begin{cases} \text{the line } \overline{PP_0} & \text{if } P \neq P_0 \\ \text{the ``tangent line'' at } P_0, & \text{if } P = P_0 \end{cases}$$

$$= \left(\frac{\partial f}{\partial x_0}(P_0) : \frac{\partial f}{\partial x_1}(P_0) : \frac{\partial f}{\partial x_2}(P_0) \right).$$

Remarks. We observe the following:

- It is unnecessary to assume in the theorem that f is smooth at P_0 (i.e. that $\left(\frac{\partial f}{\partial x_0}(P_0), \frac{\partial f}{\partial x_1}(P_0), \frac{\partial f}{\partial x_2}(P_0)\right) \neq (0,0,0)$, making the tangent line well-defined), since if a *conic* isn't smooth, then it is the union of two lines, and hence not absolutely irreducible.
- Observe that the tangent line at P_0 actually does pass through the point P_0, by *Euler's identity*: For homogeneous f,

$$x_0 \frac{\partial f}{\partial x_0} + \cdots + x_n \frac{\partial f}{\partial x_n} = (\deg f) \cdot f \ .$$

- The theorem needs to have a point on $X(k)$ in order to work. So although the theorem is true over any field, it is particularly nice over finite fields, as then the Chevalley–Warning theorem gives us the existence of a point.

Suppose k is algebraically closed, and $f, g \in k[x_0, x_1, x_2]$ are homogeneous polynomials without a common factor. Let δ_P to be the *intersection multiplicity* of f and g at the point $P \in \mathbb{P}^2(k)$; if we do a linear change of variables so that P becomes $(1 : 0 : 0)$, this

may be defined as the dimension of a k-vector space:

$$\delta_P = \dim_k \frac{k[[x,y]]}{(f(1,x,y), g(1,x,y))} \ .$$

(In particular, if $f(P) = g(P) = 0$ and f and g are both smooth at P, and the tangents to f and g at P are different, then $\delta_P = 1$.) For convenience, define $\delta_P = 0$ if $f(P)$, $g(P)$ are not both zero. Then we have:

Theorem 2.7 (Bézout's Theorem)**.** *For f, g as above,*

$$\sum_{P \in \mathbb{P}^2(k)} \delta_P = \deg(f) \cdot \deg(g) \ .$$

3. Week Three

Proposition 3.1. *Suppose we have*

$$f(x_1, \ldots, x_n) \in \mathbb{F}_q(x_1, \ldots, x_n) \quad f \neq 0, \deg f = d \ .$$

Then

$$N(f) = \#\{(a_1, \ldots, a_n) \in \mathbb{F}_q | f(a_1, \ldots, a_n) = 0\} \leq ndq^{n-1}.$$

We will look at solutions in n space, slicing it with hyperplanes. The proof is by induction on n.

Proof. In the case $n = 1$, we have $f(x_1) = 0, \deg f = d$ so $N(f) \leq d = d \cdot 1 \cdot q^{1-1}$ and the proposition is true for $n = 1$. Now assume the bound for $n - 1$. For each $a \in \mathbb{F}_q$, look at $f_a = f(a, x_2, \ldots, x_n) = 0$.

$$N(f) = \sum_{a \in \mathbb{F}_q} N(f_a)$$

where $\deg f_a \leq d$ for all a. If $f_a \neq 0$, we can apply induction and get

$$N(f_a) \leq d(n-1)q^{n-2}.$$

If $f_a = 0$, then $N(f_a) = q^{n-1}$. Now, $f_a = 0$ if and only if $(x_1 - a)|f$, but this can happen for at most d values of a (since as a polynomial in x_1, $\deg f \leq d$). Then

$$N(f) = \sum_{a \in \mathbb{F}_q} N(f_a) = \sum_{f_a \neq 0, a \in \mathbb{F}_q} N(f_a) + \sum_{f_a = 0, a \in \mathbb{F}_q} N(f_a) \leq d(n-1)q^{n-2}q + dq^{n-1} = dnq^{n-1}$$

□

One would expect a bound of the type dq^{n-1}. If f is a product of d disjoint hyperplanes,

$$f(x_1, \ldots, x_n) = (x_1 - \alpha_1) \ldots (x_1 - \alpha_d) \ ,$$

then we reach the bound; $N(f) = dq^{n-1}$.

For $n = 2$, the proposition gives $N(f) \leq 2dq$. We will do better:

Proposition 3.2. *If $f(x,y) \in \mathbb{F}_q(x,y), f \neq 0, \deg f = d$, then $N(f) \leq d(q+1) + 1$.*

Proof. Without loss of generality, we assume $N(f) > 0$ and take a point $P = (a, b) \in \mathbb{F}_q$ with $f(a, b) = 0$, and look at the lines through (a, b). There are $q + 1$ such lines. Let $L_1, \ldots, L_k$ be the lines through (a, b) such that the equation of L_i divides f. $l_1 \ldots l_k | f$ so $f = l_1 \ldots l_k g, \deg g = d - k$.

$$N(f) = 1 + (q-1)k + \#(c, d) \in \mathbb{F}_q^2 \setminus \cup l_i | g(c, d) = 0 \ .$$

Where 1 counts the point P and $(q-1)k$ count the $q-1$ solutions on each line. If l is a line through P with $l \neq l_i, i = 1, \ldots, k$ then

$$\#l \cap \{g = 0\} \leq d - k.$$

$$\begin{aligned} N(f) &\leq 1 + (q-1)k + (q+1-k)(d-k) \\ &= 1 + (q-1)k + (q+1)d - (q+1)k - kd + k^2 \\ &= 1 + (q+1)d - 2k + k^2 - dk \leq 1 + (q+1)d \end{aligned}$$

because $0 \leq k \leq d$. □

Exercise 3.1. If f is irreducible, show that $N(f) \leq (q+1)(d-1)$.

Example 3.3. (The Hermitian Curve) The curve over $\mathbb{F}_{q^2}$ defined by

$$y^q + y - x^{q+1} = 0$$

has degree $q + 1$, is absolutely irreducible (apply Eisenstein to it as a polynomial in x, in $\mathbb{F}_q[y]$ using the prime y), and $N(f) = q^3$ over $\mathbb{F}_{q^2}$. That is, $N(f) = (\deg f - 1) \cdot \#\mathbb{F}_{q^2}$.

Proof. Consider the Trace and the Norm,

$$\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) = \alpha + \alpha^q + \cdots + \alpha^{q^{n-1}}$$

$$N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) = \alpha \cdot \alpha^q \cdot \cdots \cdot \alpha^{q^{n-1}} = \alpha^{\frac{q^n-1}{q-1}}$$

□

Lemma 3.4. (1) *For all* $a \in \mathbb{F}_q$, $\#\{\alpha \in \mathbb{F}_{q^n} | Tr(\alpha) = a\} = q^{n-1}$.
(2) *For all* $a \in \mathbb{F}_q^*$, $\#\{\alpha \in \mathbb{F}_{q^n}^* | N(\alpha) = a\} = \frac{q^n-1}{q-1}$.

Given $\alpha \in \mathbb{F}_{q^2}$, $\alpha^{q+1} = N(\alpha) \in \mathbb{F}_q$. There are q elements $\beta \in \mathbb{F}_{q^2}$ such that $\beta^2 + \beta = Tr(\beta) = N(\alpha)$ (by the Lemma), so we get $q^2 \cdot q = q^3$ points (α, β) on $f = 0$.

Proof. (1) Trace is a homomorphism under addition. Assertion (1) is equivalent to saying Trace is surjective and $\#\ker \mathrm{Tr} = q^{n-1}$. Now,

$$\ker \mathrm{Tr} = \{\alpha \in \mathbb{F}_{q^n} | \alpha + \alpha^q + \cdots + \alpha^{q^{n-1}} = 0\} \subseteq \{\alpha \in \bar{\mathbb{F}_q} | \alpha + \alpha^q + \cdots + \alpha^{q^{n-1}} = 0\}.$$

The last set has cardinality q^{n-1} because $x + x^q + \cdots + x^{q^{n-1}}$ is a seperable polynomial of degree q^{n-1}. So, $\#\ker \mathrm{Tr} \leq q^{n-1}$. $\mathrm{Im}\,\mathrm{Tr} \subseteq \mathbb{F}_q$ so $\#\mathrm{Im}\,\mathrm{Tr} \leq q$.

The result follows since $\#\ker \mathrm{Tr} \,\#\,\mathrm{Im}\,\mathrm{Tr} = q^n$ (because $0 \to \ker \mathrm{Tr} \to \mathbb{F}_{q^n} \to \mathrm{Im}\,\mathrm{Tr} \to 0$ is exact).

The Proof of (2) is similar. □

Remark. There is a change of variables on the hermitian curve that gives $x^{q+1} + y^{q+1} = 1$.

Proposition 3.5. *If $f \in \mathbb{F}_q(x, y)$ is of degree d, and is irreducible, but not absolutely irreducible, then*

$$N(f) \leq \frac{d^2}{4}.$$

Proof. Take an absolutely irreducible factor, g, of f over $\bar{\mathbb{F}}_q$; $f = gh$. Let σ be an element of the galois group, $\sigma \neq 1$, such that $g^\sigma \neq g$. Such a σ exists because $g \notin \mathbb{F}_q(x, y)$. Now, apply σ to $f = gh$:

$$f = f^\sigma = g^\sigma \cdot h^\sigma$$

so g^σ is also a factor of f. Let $k = g \cdot g^\sigma \dots g^{\sigma^{r-1}}$ for some minimal r with $g^{\sigma^r} = g$. $k^\sigma = k$ so $k \in \mathbb{F}_q(x, y)$, and since $k|f$, we get $f = k = g \cdot g^\sigma \dots g^{\sigma^{r-1}}$.

Suppose $f(a, b) = 0$ for some $(a, b) \in \mathbb{F}_q(x, y)$. Then

$$\prod_{i=0}^{r-1} g^{\sigma^i}(a, b) = 0 \ .$$

For some i, $0 = g^{\sigma^i}(a, b) = g(a, b)^{\sigma^i}$ which implies $g(a, b) = 0$, so $g^\sigma(a, b) = 0$. Note that $\deg g = \deg g^\sigma$; all galois conjugates have the same degree, and there are r of them. g is irreducible, so that g and g^σ have no common factor, so by Bezout, there are at most $\frac{d^2}{r^2} \leq \frac{d^2}{4}$ common solutions. □

3.1. **Basic Notions from Algebraic Geometry.** Let $k = \overline{\mathbb{F}_q}$, the algebraic closure of $\mathbb{F}_q$.

Suppose $f_1, \dots, f_m \in k[x_1, \dots, x_n]$. Let X be the set

$$X = \{(a_1, \dots, a_n) \in k^n | f_j(a_1, \dots, a_n) = 0 j = 1, \dots, m\} \ .$$

This is called an algebraic set. Let

$$I(X) = (f_1, \dots, f_m) \subseteq k[x_1, \dots, x_n]$$

be the ideal generated by $f_1, \dots, f_m$. For an ideal I in $k[x_1, \dots, x_n]$, define the radical of I as the ideal $\sqrt{I} = \{g \in k[x_1, \dots, x_n] \mid \exists r \geq 1, g^r \in I\}$.

Theorem 3.6 (Hilbert Nullstellensatz)**.** *Suppose X is an algebraic set defined by the ideal $I \subseteq k[x_1, \dots, x_n]$. Then*

$$\{f \in k[x_1, \dots, x_n] \mid f(a_1, \dots, a_n) = 0, \forall (a_1, \dots, a_n) \in X\} = \sqrt{I}.$$

This is true for any algebraically closed field.

If an ideal satisfies $I = \sqrt{I}$ we call it a radical ideal. $R_X = k[x_1, \dots, x_n]/I(X)$ is called the coordinate ring of X.

Definition 3.7. An algebraic set X is irreducible if $X = Y \cup Z$, Y, Z algebraic sets, implies $Y \subseteq Z$ or $Z \subseteq Y$.

Fact 3.8. *X is irreducible if and only if $I(X)$ is a prime ideal if and only if R_X is an integral domain.*

Fact 3.9. *Every algebraic set is a finite union of irreducible algebraic sets in a unique way. Those irreducible algebraic sets are called components of X.*

Definition 3.10. An irreducible algebraic set is called an *algebraic variety.*

More precisely, it is an affine algebraic variety, as we are working in k^n (affine space). Later we will also consider projective space.

For X irreducible, K_X, the field of fractions of R_X, is called the function field of X.

Definition 3.11 (Dimension Definition 1)**.** Suppose X is an algebraic variety. Then $\dim X$ is the transcendence degree of K_X over k.

Example 3.12.

$$X \subseteq k^2, \quad I = (f), X = \{f(x,y) = 0\} \quad R_X = k[x,y]/(f(x,y))$$

$K_X = k(x,y)$ subject to $f(x,y) = 0$. X has dimension 1 because x and y are related by $f(x,y) = 0$.

If we let $d = \dim X$, K_X is a finite extension of k, $K_X = k(t_1, \ldots, t_d)$ for some algebraically independent $t_1, \ldots, t_d$.

Definition 3.13 (Dimension Definition 2)**.** For X an algebraic variety, $\dim X \geq d$ if there exist $Y_0 \subsetneqq Y_1 \subsetneqq \cdots \subsetneqq Y_d = X$ where the $Y_i's$ are algebraic varieties.

We state the following without proof:

Fact 3.14. *Definition 3.11 and Definition 3.13 are equivalent.*

If X is defined over $\mathbb{F}_q$ then $\#X(\mathbb{F}_q)$ should be roughly of size q^d where $d = \dim X$. We will later prove that if X is an absolutely irreducible algebraic variety, then

$$\lim_{n\to\infty} \frac{\log \#X(\mathbb{F}_{q^n})}{n \log q} = d \ .$$

Definition 3.15. Suppose X is an algebraic variety defined by $f_1 = f_2 = \cdots = f_m = 0$. Given a point $x \in X$ we say X is *smooth* at x if the rank $\mathrm{rk}(\frac{\partial f_i}{\partial x_j}(x)) = n - \dim X$. In this case, $\ker(\frac{\partial f_i}{\partial x_j}(x))$ is called the tangent space to X at x. Finally, X is smooth if it is smooth at x for all $x \in X$.

Example 3.16.

$$f(x,y) \in k^2, f(x,y) = 0, f(0,0) = 0$$

X is smooth at $(0,0)$ if and only if

$$(\frac{\partial f}{\partial x}(0,0), \frac{\partial f}{\partial y}(0,0)) \neq (0,0) \ .$$

Example 3.17.

$$\begin{aligned} f(x,y) &= y^2 - (x^3 + x^2) \\ \frac{\partial f}{\partial x} &= -3x^2 - 2x \\ \frac{\partial f}{\partial y} &= 2y \end{aligned}$$

This is not smooth; both partials vanish at $(0,0)$. Geometrically, the curve has a node at $(0,0)$.

Example 3.18.

$$\begin{aligned} f(x,y) &= y^2 - x^3 \\ \frac{\partial f}{\partial x} &= -3x^2 \\ \frac{\partial f}{\partial y} &= 2y \end{aligned}$$

Again, this is not smooth; both partials vanish at $(0,0)$. Geometrically, this curve has a cusp at $(0,0)$.

4. Week Four

4.1. **Zeta Functions.** We first introduce some necessary notation. We will write $\mathbb{A}^n$ to denote n-dimensional affine space. So $\mathbb{A}^n(k)$ will be k^n for any field k. Let X be an algebraic variety defined over $\mathbb{F}_q$ in $\mathbb{A}^n$. This means that X is defined by an ideal $(f_1, f_2, ..., f_m)$ in $\overline{\mathbb{F}}_q[x_1, x_2, ..., x_n]$, where $f_1, f_2, ..., f_m \in \mathbb{F}_q[x_1, x_2, ..., x_n]$. Note that since X is an algebraic variety, we are already assuming that the ideal is prime. Also, we need to consider the algebraic closure $\overline{\mathbb{F}}_q$ in order to have absolute irreduciblity, but we are really only concerned with $\mathbb{F}_q$.

We can think of X as the set of solutions over $\overline{\mathbb{F}}_q$ to the system of equations $f_j = 0$, $j = 1, 2, ..., m$. So, for any field k containing $\mathbb{F}_q$, we will denote by $X(k)$ the set

$$\{(a_1, a_2, ..., a_n) \in k^n | f_j(a_1, a_2, ..., a_n) = 0 \quad 1 \leq j \leq m\} \ .$$

For instance, $X(\mathbb{F}_q)$ is the set of $\mathbb{F}_q$-rational points of X. Recall that our purpose is to study the size of the set and notice that the geometry influences the arithmetic. Hence, we can also look at $X(\mathbb{F}_{q^2})$, $X(\mathbb{F}_{q^3})$, etc. and see if the infinite collection of finite fields tells us something about the variety X. For this we will make use of the following item.

Definition 4.1. The *Zeta function* of X over the field $\mathbb{F}_q$ is the formal power series

$$Z_X(t) = \exp\Big(\sum_{r=1}^{\infty} \#X\big(\mathbb{F}_{q^r}\big)\frac{t^r}{r}\Big) \in \mathbb{Q}[[t]] \ .$$

We note that $0 \leq \#X(\mathbb{F}_q) \leq q^{rn}$, which tells us that the series is convergent for $|t| < q^{-n}$, but this is not terribly important for our purposes. Also, we mention that the same definition can be used if we take the algebraic variety X to be in the projective space $\mathbb{P}^n$.

Example 4.2. $X = \mathbb{A}^n$. We know that $\#\mathbb{A}^n(\mathbb{F}_{q^r}) = q^{nr}$, so we have

$$\begin{aligned} Z_{\mathbb{A}^n}(t) &= \exp\Big(\sum_{r=1}^{\infty} q^{nr}\frac{t^r}{r}\Big) \\ &= \exp\Big(\sum_{r=1}^{\infty} \frac{(q^n t)^r}{r}\Big) \\ &= \exp\big(-\log(1-q^n t)\big) \\ &= \exp\big(\log(1-q^n t)^{-1}\big) \\ &= \frac{1}{1-q^n t} \end{aligned}$$

Notice that the information given by the zeta function is equivalent to the fact that $\#\mathbb{A}^n(\mathbb{F}_{q^r}) = q^{nr}$.

Example 4.3. $X = \mathbb{P}^n$. We have already shown that

$$\#\mathbb{P}^n(\mathbb{F}_{q^r}) = q^{nr} + q^{(n-1)r} + ... + q^r + 1 \ ,$$

therefore, by calculations similar to those made in example 1,

$$Z_{\mathbb{P}^n}(t) = \frac{1}{(1-t)(1-qt)...(1-q^n t)} \ .$$

Example 4.4. $X \subseteq \mathbb{A}^3$ is given by $x_1x_2x_3 - 1 = 0$. We notice that none of the x_i's can be zero, and the third is dependent on the other two, eg. $x_3 = 1/x_1x_2$. Therefore

$$\begin{aligned} \#X(\mathbb{F}_{q^r}) &= (q^r - 1)^2 \\ &= q^{2r} - 2q^r + 1 \ , \end{aligned}$$

and the same sort of calculations as before lead to

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

Example 4.5. The proof of this example will be given later. Consider the variety X : $y^2 + y = x^3$, and take $X \subseteq \mathbb{A}^2$ to be defined over $\mathbb{F}_2$. We will eventually show that

$$\#X(\mathbb{F}_{2^n}) = \begin{cases} 2^n & \text{if } n \text{ is odd} \\ 2^n - 2(-2)^{n/2} & \text{if } n \text{ is even} \ . \end{cases}$$

So for any n,

$$\#X(\mathbb{F}_{2^n}) = 2^n - (\sqrt{-2})^n - (-\sqrt{2})^n.$$

Notice that if n is odd then $3 \nmid 2^n - 1$. So cubing is an automorphism of $\mathbb{F}_{2^n}^*$, that is, the map $x \to x^3$ is a bijection on $\mathbb{F}_{2^n}$. Also,

$$\#\{x \in \mathbb{A}_{2^n} \mid \mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}(x) = 0\} = 2^{n-1} \ .$$

So the case when n is odd is simple. The other case, however, is more difficult. For instance, consider $X(\mathbb{F}_4)$. Of course, $0^3 = 0$, but for $x \neq 0, x \in \mathbb{F}_4$ we have $x^3 = 1$. For

each of these, there exist two values for y in $\mathbb{F}_4$ with $y^2 + y = x^3$. So $\#X(\mathbb{F}_4) = 8 = 2^2 - 2(-2)^1$.

If instead we consider $X(\mathbb{F}_{16})$, we notice that $(x^3)^5 = 1$ for all $x \neq 0$. So the cubes are actually the fifth roots of unity. Now,

$$z^5 - 1 = (z-1)(z^4 + z^3 + z^2 + z + 1) \ ,$$

therefore, if $z^5 = 1$ and $z \neq 1$, then $\mathrm{Tr}_{\mathbb{F}_{16}/\mathbb{F}_2}(z) = 1$ while $\mathrm{Tr}_{\mathbb{F}_{16}/\mathbb{F}_2}(1) = 0$. So we only get points on the curve when $x^3 = 1$. Therefore it follows that $X(\mathbb{F}_{16}) = X(\mathbb{F}_4)$ and $\#X(\mathbb{F}_{16}) = 8 = 16 - 2(-2)^2$. If we assume the formula for all n we get

$$Z_X(t) = \frac{1 + 2t^2}{(1-t)(1-2t)} \ .$$

4.2. **Weil Conjectures.** We will first state the Weil Conjectures with a bit of explanation, then present the motivation for them.

Theorem 4.6. *Let X be an algebraic variety defined over $\mathbb{F}_q$ and let $Z_X(t)$ be its zeta function. Then $Z_X(t)$ is a rational function with rational coefficients. That is, $Z_X(t) \in \mathbb{Q}(t)$.*

Note that this means

$$Z_X(t) = \frac{A(t)}{B(t)}$$

with $A(t), B(t) \in \mathbb{Q}[t]$. Of course, we could multiply through by the least common multiple of the denominators of the coefficients to get our functions $A(t), B(t) \in \mathbb{Z}[t]$. Notice that the zeta function, being an exponential, must have a constant term of 1. Therefore, we can make $A(0) = B(0) = 1$. Factoring, we get

$$Z_X(t) = \frac{(1-\alpha_1 t)(1-\alpha_2 t)...(1-\alpha_s t)}{(1-\beta_1 t)(1-\beta_2 t)...(1-\beta_u t)} \qquad \alpha_i, \beta_i \in \mathbb{C},$$

which is equivalent to saying that

$$\#X(\mathbb{F}_{q^r}) = \sum_{i=1}^{s} \alpha_i^r - \sum_{j=1}^{u} \beta_j^r$$

for all $r \geq 1$.

This part of the conjectures was proved for curves by F.K. Schmidt in the 1920's and was proved in general by Dwork around 1959.

We mention one consequence of this before we proceed. If we know the α_i's and the β_j's, we can find $X(\mathbb{F}_{q^r})$ for all r. In order to know the α's and β's, it is enough to know $\#X(\mathbb{F}_{q^r})$ for $r \leq s + u$. So this is nice if we happen to know s and u in advance. We will return to this case later.

Theorem 4.7. *Suppose X is as in the hypotheses of conjecture 4.6 with the added conditions that X is smooth and projective of dimension d, then*

$$Z_X(t) = \frac{P_1(t)P_3(t)...P_{2d-1}(t)}{P_0(t)P_2(t)...P_{2d-2}(t)P_{2d}(t)}$$

where each $P_i(t) \in \mathbb{Z}[t]$, *and* $P_i(0) = 1$.

Further,

$$Z_X\Big(\frac{1}{q^n t}\Big) = \pm (q^n)^{\chi/2} t^\chi Z_X(t)$$

where $\chi = \sum_{i=0}^{2d} (-1)^i \deg P_i$.

If X *is the reduction modulo* p *of a smooth projective variety* $\widetilde{X}$ *over* $\mathbb{Q}$, *then* $\deg P_i$ *is the* i*th Betti number of* $\widetilde{X}(\mathbb{C})$. *That is*

$$\deg P_i = \dim_{\mathbb{R}} H^i(X(\mathbb{C}), \mathbb{R}).$$

Note that, for the last part, $\widetilde{X}(\mathbb{C})$ is a manifold of complex dimension d, thus of real dimension $2d$.

This part of the conjectures was proved for curves by Schmidt in the 1920's and proved in general by Grothendieck in the 1960's.

Theorem 4.8. *Under the same hypotheses and notation as in 4.7,*

$$P_i(t) = \prod_{j=1}^{b_i} (1 - \alpha_{ij} t)$$

where $\alpha_{ij} \in \mathbb{C}$ *and* $|\alpha_{ij}| = q^{i/2}$.

This is called the Riemann hypothesis for varieties over finite fields and was proved for curves by Weil in 1948. It was proved in general in 1974 by Deligne. We just mention that one consequence of this is the Ramanujan-Petersson conjecture.

In order to help explain the motivation for the Zeta function and the Weil conjectures, we will explore a bit of topology. Suppose that M is a compact, orientable, smooth, class C^∞, connected manifold of dimension d. From algebraic topology, M has cohomology groups $H^i(M, \mathbb{C})$, for $0 \le i \le d$, which are finite dimensional $\mathbb{C}$ vector spaces. Also, $\dim(H^i(M, \mathbb{C})) = b_i$, the ith Betti number of M so that $b_0 = b_d = 1$ and, due to Poincaré duality,

$$H^i(M, \mathbb{C})^* \simeq H^{d-i}(M, \mathbb{C})$$

For example, if we have a 2-manifold of genus g, then $H^0 = H^2 = \mathbb{C}$ while $\dim H^1 = 2g$. We also know that the Euler characteristic of M is $\chi(M) = \sum_{i=0}^{d} (-1)^i b_i$.

We need to state one theorem before we proceed.

4.3. **Lefschetz' Fixed Point Theorem.** Suppose that we have a diffeomorphism $f : M \to M$ which is orientation preserving, and assume that, for all P with $f(P) = P$, df_P has no eigenvalue equal to 1. Then

$$\#\{P \in M | f(P) = P\} = \sum_{i=0}^{d} (-1)^i \operatorname{Tr}(f^* \text{ on } H^i),$$

where

$$f^* : H^i(M, \mathbb{C}) \to H^i(M, \mathbb{C}), \qquad i = 0, 1, ..., d$$

are linear maps induced by the diffeomorphism.

So the theorem states, in particular, that although the traces are in $\mathbb{C}$, the alternating sum happens to be an integer, and the sum gives us the number of fixed points. If we compose f with itself n times, we can also consider the fixed points of f^n, and the theorem gives us

$$\#\{P \in M | f^n(P) = P\} = \sum_{i=0}^{d} (-1)^i \operatorname{Tr}[(f^*)^n on\ H^i].$$

To this we will apply the following lemma.

Lemma 4.9. *If $\varphi : V \to V$ is a linear map on the finite dimensional $\mathbb{C}$ vector space V, then*

$$\det(I - t\varphi)^{-1} = \exp(\sum_{n=1}^{\infty} \operatorname{Tr}(\varphi^n)\frac{t^n}{n}).$$

So we can write

$$\begin{aligned}\exp \sum_{n=1}^{\infty} \#\{P \in M | f^n(P) = P\}\frac{t^n}{n} &= \prod_{i=0}^{d} (\exp(\sum_{n=1}^{\infty} [\operatorname{Tr}(f^*)^n \text{ on } H^i]\frac{t^n}{n})^{(-1)^i} \\ &= \prod_{i=0}^{d} \det(I - t[f^* \text{ on } H^i])^{(-1)^{i+1}},\end{aligned}$$

and this is now in $\mathbb{Q}(t)$.

4.4. **Rational points as fixed points of the Frobenius map.** Suppose that X is an algebraic variety over $\mathbb{F}_q$. We can think of X as lying inside of $\mathbb{A}^n$ or $\mathbb{P}^n$.

Definition 4.10. The $\mathbb{F}_q$ *Frobenius map* F on $\mathbb{A}^n/\overline{\mathbb{F}}_q$ is given by

$$F((a_1, a_2, ..., a_n)) = (a_1^q, a_2^q, ..., a_n^q).$$

On $\mathbb{P}^n/\overline{\mathbb{F}}_q$ the map is given by

$$F((a_0 : a_1 : ... : a_n)) = (a_0^q : a_1^q : ... : a_n^q).$$

We wish to investigate the fixed points of this map. That is, we wish to understand what it means for $F^m(P) = P$. Over $\mathbb{A}^n$, we can write

$$\begin{aligned}(a_1^{q^m}, a_2^{q^m}, ..., a_n^{q^m}) = (a_1, a_2, ..., a_n) &\Leftrightarrow a_i^{q^m} = a_i \qquad i = 1, 2, ..., n \\ &\Leftrightarrow a_i \in \mathbb{F}_{q^m} \qquad i = 1, 2, ..., n \\ &\Leftrightarrow P \in \mathbb{A}^n(\mathbb{F}_{q^m}).\end{aligned}$$

The same can be done in projective space up to constant multiples of the point P. But we are really concerned with what happens on the variety X. The following Lemma gives us the answer.

Lemma 4.11. *If X is an algebraic variety defined over $\mathbb{F}_q$, then F maps X to X.*

Proof. Let X be defined over $\mathbb{F}_q$, then X is the zero set of a system of polynomials $f_1, f_2, ..., f_r \in \mathbb{A}_q[x_1, x_2, ..., x_n]$.

Recall that q is a power of the characteristic of the field $\mathbb{F}_q$, and the coefficients of f_j are in $\mathbb{F}_q$. If P is in X, then $P = (a_1, a_2, ..., a_n)$ and $f_j(P) = 0$ for all $j = 1, 2, ..., r$. So, $f_j(P)^q = 0$. But $f_j(P)^q = f_j(F(P))$ so $f_j(F(P)) = 0$, that is, $F(P) \in X$. □

We should also mention that if we write the Zeta function as

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

where we have $2d$ polynomials because $\mathbb{C}$ is of dimension 2 over $\mathbb{R}$, then P_i is the characteristic polynomial of the Frobenius map in $H^i(X, K)$, with K being a field. Further, $H^i(X, K)$ is dual to $H^{2d-i}(X, K)$. Note that

$$P_i(t) = \prod_{j=1}^{b_i} (1 - \alpha_{ij} t)$$

where $|\alpha_{ij}| = q^{i/2}$, and $\{q^d/\alpha_{i,j}\} = \{\alpha_{2d-i,j}\}$ because the cohomology has this Poincaré duality. For more information on this topic, we refer the reader to Katz's Arizona Winter School 2000 notes.[1]

One final consequence of the Weil conjectures is that

$$\#X(\mathbb{F}_{q^r}) = \sum_{i=0}^{2d} (-1)^i \sum_{j=1}^{b_i} {\alpha_{ij}}^r$$

which is equivalent to writing

$$Z(t) = \prod_{i=0}^{2d} \prod_{j=1}^{b_i} (1 - \alpha_{ij} t)^{(-1)^{i+1}} \ .$$

Further, $b_0 = b_{2d} = 1$, so we can write

$$\#X(\mathbb{F}_{q^r}) = q^{dr} + \sum_{i=0}^{2d-1} (-1)^i \sum_{j=1}^{b_i} \alpha_{ij}^r \ ,$$

which gives us the following corollary.

Corollary 4.12 (Lang-Weil)**.** *Assuming the conditions and notation under which we have been working,*

$$|\#X(\mathbb{F}_{q^r}) - q^{dr}| \leq C q^{(d-1/2)r} \ ,$$

where $C = \sum_{i=0}^{2d-1} b_i$.

Now, for curves we have $d = 1$, so we are dealing with just 3 cohomology groups: H^0, H^1, and H^2. Both H^0 and H^2 are one dimensional. Therefore

$$Z(t) = \frac{P_1(t)}{(1-t)(1-qt)}$$

[1]Available on the world wide web at http://swc.math.arizona.edu/~swcenter/aws2000/Notes.html.

with $\deg P_1 = 2g$, g being the genus of the curve. So we have

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

with $|\alpha_j| = q^{1/2}$ and

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

5. Week Five

5.1. **Arithmetical Interlude.** The Riemann Zeta-Function is defined, for all complex s with $\mathrm{Re}(s) > 1$, by

$$\zeta(s) := \sum_{n=1}^{\infty} n^{-s} \ .$$

Further, if we observe that, for all primes p,

$$\Big(1 - \frac{1}{p^s}\Big)^{-1} = \frac{1}{1 - \frac{1}{p^s}} = \sum_{m=0}^{\infty} \frac{1}{p^{ms}} \ ,$$

then by unique factorization, we have

$$\zeta(s) = \prod_p \Big(1 - \frac{1}{p^s}\Big)^{-1}$$

where the product is taken over all primes p.

These results were first proved by Euler, but it was Riemann who discovered the analytic continuation of $\zeta(s)$ to $\mathbb{C} \setminus \{1\}$ with pole at 1 of order one and residue one.

Of great importance is

Conjecture 5.1 (Riemann Hypothesis)**.** *All zeroes of the Riemann Zeta-Function* $\zeta(s)$ *in the critical strip* $0 < \mathrm{Re}(s) < 1$ *are on the line* $\mathrm{Re}(s) = \frac{1}{2}$.

Now consider the following diagram

$$\begin{array}{ccc} \mathcal{O}_K & \subseteq & K \\ \Big| & & \Big| \\ \mathbb{Z} & \subseteq & \mathbb{Q} \end{array}$$

where $\big[K : \mathbb{Q}\big] < \infty$.

Here, $\mathcal{O}_K$ denotes the ring of algebraic integers of K,

$$\mathcal{O}_K = \big\{\alpha \in K \mid \alpha^n + a_1\alpha^{n-1} + \cdots + a_n = 0, a_i \in \mathbb{Z}\big\} \ .$$

Then $\mathcal{O}_K$ is a Dedekind ring — that is, $\mathcal{O}_K$ is Noetherian and integrally closed with every prime ideal maximal. As an analogue to unique factorization over $\mathbb{Z}$, every ideal I in a Dedekind ring can be written uniquely as $I = P_1^{\alpha_1} \cdots P_k^{\alpha_k}$ where the P_i's are prime

and the α_i's are positive integers. We can then ask the question, "Are there infinitely many primes ideals in a Dedekind ring?"

This leads to the definition of the Dedekind zeta-function

$$\zeta_{\mathcal{O}_K}(s) = \sum_{\substack{I \neq 0 \\ I \subset \mathcal{O}_K}} \frac{1}{(NI)^s}$$

where $NI = \#\mathcal{O}_K/I$, the number of elements in the quotient ring $\mathcal{O}_K/I$.

It turns out that many theorems which hold for the Riemann Zeta Function also hold for $\zeta_{\mathcal{O}_K}(s)$, so the notion turns out to be fruitful over a general number field.

5.2. **Analogy Between Number Fields and Function Fields.** We can compare $\mathbb{Z}$ with the polynomial ring $k[x]$. Both are Euclidean rings, and in $k[x]$ the irreducible polynomials play the role of prime numbers. We have, by analogy with number fields,

$$\begin{array}{ccc} \mathcal{O}_K & \subseteq & K \\ | & & | \\ k[x] & \subseteq & k(x) \end{array}$$

where $K = k(x, y)$ is the field of fractions of $k[x, y]/(f(x, y)) \subseteq \mathcal{O}_K$ and $f(x, y) = 0$ determines the extension K.

We would like to imitate the definition of the Dedekind Zeta Function for function fields instead of number fields. In order for this to work, we need $\mathcal{O}_K/I$ to be finite for all nonzero ideals I, and this in turn forces k to be finite. Then the same definition will hold, but unfortunately, there is no canonical choice for $\mathcal{O}_K$.

Consider

$$\zeta_{\mathbb{F}_q[x]}(s) = \sum_{I \neq 0} \frac{1}{(NI)^s} = \sum_{\substack{f(x) \in \mathbb{F}_q[x] \\ f(x) \text{ monic}}} \frac{1}{(N(f))^s} \ .$$

The quotient ring $k[x]/(f(x))$ is in bijection with $\{a(x) \in k[x] \mid \deg(a) < \deg(f)\}$ by the map sending every polynomial in $k[x]$ to its remainder upon division by f. Therefore $N(f)$ is the number of polynomials of degree less than $\deg f$, that is $N(f) = q^{\deg f}$. Using the fact that for each fixed d there are exactly q^d monic polynomials of degree d, we get

$$\sum_{\substack{f(x) \in \mathbb{F}_q[x] \\ f(x) \text{ monic}}} \frac{1}{(N(f))^s} = \sum_{\substack{f(x) \in \mathbb{F}_q[x] \\ f(x) \text{ monic}}} \frac{1}{q^{s \deg f}} = \sum_{d=0}^{\infty} \frac{q^d}{q^{sd}} = \frac{1}{1 - q^{1-s}}.$$

Observe that the final equality implies that $\zeta_{\mathbb{F}_q[x]}(s)$ has no zeroes, unlike $\zeta(s)$. Also, if we recall that

$$Z_{\mathbb{A}^n/\mathbb{F}_q}(t) = \frac{1}{1 - q^n t}$$

then

$$\zeta_{\mathbb{F}_q[x]}(s) = Z_{\mathbb{A}^1/\mathbb{F}_q}(q^{-s})$$

Also,

$$\zeta_{\mathbb{F}_q[x]}(s) = \prod_p \Big(1 - \frac{1}{q^{s \deg p}}\Big)^{-1} = \prod_{d=1}^{\infty} \Big(1 - \frac{1}{q^{sd}}\Big)^{-a_d}$$

where p is monic and irreducible and a_d is the number of monic irreducible polynomials of degree d. Then, replacing q^{-s} by t, we obtain

$$\frac{1}{1-qt} = \prod_{d=1}^{\infty} (1-t^d)^{-a_d}$$

so that by taking logarithms,

$$-\log(1-qt) = \log\left(\prod_{d=1}^{\infty}(1-t^d)^{-a_d}\right) = \sum_{d=1}^{\infty} -a_d \log(1-t^d)\ .$$

Then differentiating with respect to t, we arrive at

$$\frac{q}{1-qt} = \sum_{d=1}^{\infty} a_d \Big(\frac{dt^{d-1}}{1-t^d}\Big)\ .$$

Note also that

$$\frac{q}{1-qt} = q\sum_{r=0}^{\infty}(qt)^r$$

and

$$\sum_{d|m} d a_d = q^m\ .$$

To see the latter equalities, note that we can factor $x^{q^m} - x = \prod_{\substack{p \text{ irreducible} \\ \deg p | m}} p$ because a root of $p \mid x^{q^m} - x$ must be in $\mathbb{F}_{q^m}$, and conversely, if $\deg(p) \mid m$, then the roots of p must belong to $\mathbb{F}_{q^m}$

Using Möbius inversion, we get an analogue of the Prime Number Theorem:

$$a_m = \frac{1}{m}\sum_{d|m} \mu\Big(\frac{m}{d}\Big) q^d \sim \frac{q^m}{m}$$

where μ is the Möbius function.

Now suppose $X \subseteq \mathbb{A}^n$, X a smooth curve defined over $\mathbb{F}_q$, i.e., $\exists f_1, \cdots, f_m \in \mathbb{F}_q[x_1, \cdots, x_n]$ such that X is the set of common zeroes in $\overline{\mathbb{F}_q}^n$.

Consider $R = \mathbb{F}_q[x_1, \cdots, x_n]/(f_1, \cdots, f_m)$ and let K be the field of fractions for R. Suppose $X \supseteq Y$ and Y is irreducible. The ideal P of Y in $\mathbb{F}_q[x_1, \cdots, x_n]$ contains $(f_1, \cdots, f_m)$. But Y irreducible implies that P is prime, so the image of P is prime in R. We can also invert the process to get prime ideals in $\mathbb{F}_q[x_1, \cdots, x_n]$ from prime ideals in R.

By definition, $\dim(X) = 1$ if and only if every prime ideal of R is maximal. It turns out that R is actually a Dedekind ring. Moreover, the quotients of R are finite, so we can try to define a Zeta function by

$$\zeta_R(s) = \sum_{I \neq 0} \frac{1}{(NI)^s} = \prod_{P \text{ prime}, P \neq 0} \left(1 - \frac{1}{(NP)^s}\right)^{-1}$$

As before, X is a smooth affine curve over $\mathbb{F}_q$, R = the coordinate ring of $X = \mathbb{F}_q[x_1, \ldots, x_n]/I$ where I = the ideal generated by the polynomials which determine X,

$$\zeta_R(s) = \sum_{I \neq 0} \frac{1}{(NI)^s} = \prod_{P \text{ prime, } P \neq 0} \left(1 - \frac{1}{(NP)^s}\right)^{-1}$$

$$Z_X(t) = \exp\left(\sum_{r=1}^{\infty} \#X(\mathbb{F}_{q^r}) \frac{t^r}{r}\right)$$

Theorem 5.2. $\zeta_R(s) = Z_X(q^{-s})$

Proof. Nonzero Prime ideals of R are in 1-1 correspondence with $\mathbb{F}_q-$irreducible subvarieties of X defined over $\mathbb{F}_q$. These subvarieties are $\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$-orbits of points in $X(\overline{\mathbb{F}_q})$.

This means that if $P \in X(\mathbb{F}_{q^r})$ but not in a smaller field, then P has r conjugates,

$$P = P^{(1)}, \ldots, P^{(r)},$$

where if $P = (a_1, \ldots a_n)$, $P^{(i)} = (a_1^{q^{i-1}}, \ldots, a_n^{q^{i-1}})$, the orbits of points under the Frobenius map F in $X(\overline{\mathbb{F}_q})$

If $P \in X(\mathbb{F}_{q^r})$, then if $g \in R$, the map sending g to $g(P)$ is an onto homomorphism from R to $\mathbb{F}_{q^r}$, and the kernel is a prime ideal $\mathfrak{P}$ corresponding to P. $R/\mathfrak{P} \cong \mathbb{F}_{q^r}$,so $N\mathfrak{P} = q^r$. Define $r = \deg \mathfrak{P}$, so $N\mathfrak{P} = q^{\deg \mathfrak{P}}$. Then

$$\zeta_R(s) = \prod_{\mathfrak{P}} \left(1 - \frac{1}{q^{s \deg \mathfrak{P}}}\right)^{-1}$$

and setting $t = q^{-s}$,

$$\zeta_R(s) = \prod_{\mathfrak{P}} \left(1 - t^{\deg \mathfrak{P}}\right)^{-1}.$$

Now consider $\zeta_R(s)$ as a function $F(t)$ of t. Then by logarithmic differentiation,

$$\begin{aligned}
\frac{F'(t)}{F(t)} &= \sum_{\mathfrak{P}} \frac{\deg \mathfrak{P}}{1 - t^{\deg \mathfrak{P}}} t^{\deg \mathfrak{P} - 1} \\
&= \sum_{\mathfrak{P}} \sum_{m=0}^{\infty} (\deg \mathfrak{P}) t^{\deg \mathfrak{P} - 1} t^{m \deg \mathfrak{P}} \\
&= \sum_{\mathfrak{P}} \sum_{m=0}^{\infty} (\deg \mathfrak{P}) t^{(m+1) \deg \mathfrak{P} - 1}.
\end{aligned}$$

Now set $k = (m+1)\deg \mathfrak{P}$. Then the sum becomes

$$\sum_{k=1}^{\infty}\Big(\sum_{\deg \mathfrak{P}|k} \deg \mathfrak{P}\Big)t^{k-1} = \sum_{k=1}^{\infty} N_k t^{k-1}$$

where N_k is the number of points in $X(\overline{\mathbb{F}_q})$ whose orbit under the Frobenius map has cardinality dividing k. But the degree of the field generated by the coordinates of P divides k, so $P \in X(\mathbb{F}_{q^k})$, $N_k = \#X(\mathbb{F}_{q^k})$, and

$$\log F(t) = \int_1^t \frac{F'(x)}{F(x)}dx = \sum_{k=1}^{\infty} N_k \frac{t^k}{k} \ ,$$

so

$$\zeta_R(s) = F(t) = \exp\left(\sum_{k=1}^{\infty} N_k \frac{t^k}{k}\right) = \exp\left(\sum_{k=1}^{\infty} \#X(\mathbb{F}_{q^k})\frac{t^k}{k}\right) = Z_X(t) = Z_X(q^{-s})$$

□

Consider a homomorphism $\chi : \mathbb{F}_q^* \to \mathbb{C}^*$ whose image is the n^{th}roots of unity where $n \mid q-1$, and a homomorphism $\psi : \mathbb{F}_q \to \mathbb{C}$ whose image is the pth roots of unity. Define $\chi_m : \mathbb{F}_{q^m}^* \to \mathbb{C}^*$ and $\psi_m : \mathbb{F}_{q^m} \to \mathbb{C}$ by

$$\chi_m(x) = \chi(N_{\mathbb{F}_{q^m}/\mathbb{F}_q}(x))$$

and

$$\psi_m(x) = \psi(Tr_{\mathbb{F}_{q^m}/\mathbb{F}_q}(x)) \ .$$

Define the generalized Gauss sum $g(\chi_m, \psi_m)$ as

$$g(\chi_m, \psi_m) = \sum_{x \in \mathbb{F}_{q^m}} \chi_m(x)\psi_m(x)$$

with the convention that $\chi_m(0) = 0$.

Theorem 5.3 (Hasse-Davenport formula)**.** $-g(\chi_m, \psi_m) = (-g(\chi, \psi))^m$

Before proving the theorem, we use the Hasse-Davenport formula to complete our computation of the zeta function of $y^2 - y = x^3$ over $\mathbb{F}_2$. We have already shown that $\#X(\mathbb{F}_{2^n}) = 2^n$ when n is odd. Now we will establish that $\#X(\mathbb{F}_{2^n}) = 2^n - 2(-2)^{\frac{n}{2}}$ when n is even. Since n even $\Rightarrow 2^n = 4^{\frac{n}{2}}$, we will work over $\mathbb{F}_{4^m}$

Let $u \in \mathbb{F}_{4^m}$, $u \neq 0$. Then $\chi_m(u) = 1$ if and only if u is a cube. Otherwise, $\chi_m(u) =$ the image of w or w^2 where w is a generator for $\mathbb{F}_4^*$. Then

$$1 + \chi_m(u) + \chi_m(\overline{u}) = 1 + \chi_m(u) + \overline{\chi_m(u)}$$

$$= \begin{cases} 3 & \text{if } u \text{ is a cube, } u \neq 0 \\ 0 & \text{if } u \text{ is not a cube} \\ 1 & \text{if } u = 0 \end{cases} = \#\{x \in \mathbb{F}_{4^m} \mid x^3 = u\} \ .$$

Now

$$\begin{aligned}\psi_m(u) &= (-1)^{Tr_{\mathbb{F}_{q^m}/\mathbb{F}_q}(u)} \\ &= \begin{cases} 1, \text{ if } u = y^2 + y \\ -1, \text{ otherwise} \end{cases}\end{aligned}$$

and

$$1 + \psi_m(u) = \#\{y \in \mathbb{F}_{q^m} \mid y^2 + y = u\} \ .$$

Then

$$\begin{aligned}\#X(\mathbb{F}_{4^m}) &= \sum_{u \in \mathbb{F}_{4^m}} (1 + \chi_m(u) + \overline{\chi_m(u)})(1 + \psi_m(u)) \\ &= \sum_{u \in \mathbb{F}_{4^m}} 1 + \chi_m(u) + \overline{\chi_m(u)} + \psi_m(u) + \chi_m(u)\psi_m(u) + \overline{\chi_m(u)}\psi_m(u) \ .\end{aligned}$$

Now note that

$$\sum_{u \in \mathbb{F}_{4^m}} \psi_m(u) = \sum_{u \in \mathbb{F}_{4^m}} \chi_m(u) = \sum_{u \in \mathbb{F}_{4^m}^*} \chi_m(u) = 0 \ ,$$

so that we have

$$\begin{aligned}\#X(\mathbb{F}_{4^m}) &= \sum_{u \in \mathbb{F}_{4^m}} 1 + \chi_m(u)\psi_m(u) + \overline{\chi_m(u)}\psi_m(u) \\ &= 4^m + g(\chi_m, \psi_m) + \overline{g(\chi_m, \psi_m)} \\ &= 4^m - (-g(\chi_m, \psi_m)) - (-\overline{g(\chi_m, \psi_m)}) \\ &= 4^m - (-g(\chi, \psi))^m - (-\overline{g(\chi, \psi)})^m\end{aligned}$$

by Hasse-Davenport.

Finally, if we observe that

$$\begin{aligned}g(\chi, \psi) &= \chi(1)\psi(1) + \chi(w)\psi(w) + \chi(w^2)\psi(w^2) \\ &= 1 + e^{\frac{2\pi i}{3}}(-1) + e^{\frac{4\pi i}{3}}(-1) = 2 \ ,\end{aligned}$$

we obtain

$$\#X(\mathbb{F}_{4^m}) = 4^m - 2(-2)^m = 2^{2m} - 2(-2)^m$$

as conjectured.

Now for the proof of the Hasse-Davenport formula. First, a definition.

Definition 5.4. If $f(x) \in \mathbb{F}_q[x]$ is of the form $f(x) = x^m - c_1 x^{m-1} + \ldots + (-1)^m c_m$,

$$\lambda(f) := \chi(c_n)\psi(c_1)$$

where χ, ψ are as before.

Lemma 5.5. $\lambda(fg) = \lambda(f)\lambda(g)$

The proof is trivial.

Lemma 5.6. *Suppose $u \in \mathbb{F}_{q^m}$ with minimal polynomial $f(x)$ over $\mathbb{F}_q$ of degree $d \mid m$. Then*

$$\lambda(f)^{\frac{m}{d}} = \chi_m(u)\psi_m(u)$$

Proof. Set $f(x) = x^d - a_1x^{d-1} + \ldots + (-1)^d a_d$, $a_1 = Tr_{\mathbb{F}_{q^d}/\mathbb{F}_q}(u)$, $a_d = N_{\mathbb{F}_{q^d}/\mathbb{F}_q}(u)$. Then

$$\frac{m}{d}a_1 = \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(u), a_d^{\frac{m}{d}} = N_{\mathbb{F}_{q^m}/\mathbb{F}_q}(u)$$

and

$$\begin{aligned}\chi_m(u)\psi_m(u) &= \chi(a_d^{\frac{m}{d}})\psi(\frac{m}{d}a_1)\\ &= \chi(a_d)^{\frac{m}{d}}\psi(a_1)^{\frac{m}{d}}\\ &= (\chi(a_d)\psi(a_1))^{\frac{m}{d}}\\ &= \lambda(f)^{\frac{m}{d}}\end{aligned}$$

□

Define $L(t,\lambda) := \sum_{\substack{f(x)\in\mathbb{F}_q[x]\\ f \text{ monic}}} \lambda(f)t^{\deg(f)} = \sum_{\substack{f(x)\in\mathbb{F}_q[x]\\ f \text{ monic}}} \lambda(f)\frac{1}{(N(f))^s}$ where $q^{-s} = t$, so

$$L(t,\lambda) = \sum_{d=0}^{\infty}\left(\sum_{\substack{f(x)\in\mathbb{F}_q[x]\\ \deg(f)=d\\ f \text{ monic}}}\lambda(f)\right)t^d = 1 + g(\chi,\psi)t + \{\text{higher-order terms}\}$$

since $\lambda(t-c) = \chi(c)\psi(c)$

Next time, we will prove the following:

Lemma 5.7. *The coefficients of $L(t,\lambda)$ of degree ≥ 2 vanish.*

6. Week Six

Recall that we have the following non-trivial homomorphisms: $\chi : \mathbb{F}_q^* \to \mathbb{C}^*$ a multiplicative character, and $\psi : \mathbb{F}_q \to \mathbb{C}^*$ an additive homomorphism. Also note that every element in the image of one of these homomorphisms is a root of unity. Now define

$$\chi_m = \chi \circ N_{\mathbb{F}_{q^m}/\mathbb{F}_q} \qquad \psi_m = \psi \circ \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q} \ .$$

We extend χ_m to a map on all of $\mathbb{F}_q$ by defining $\chi_m(0) = 0$. Now we define the Gauss sum to be

$$g(\chi_m,\psi_m) = \sum_{x\in\mathbb{F}_{q^m}} \chi_m(x)\psi_m(x) \ .$$

Note that $\chi_1 = \chi$ and $\psi_1 = \psi$. Eventually, we will prove

Theorem 6.1 (Hasse-Davenport Formula)**.** $-g(\chi_m,\psi_m) = (-g(\chi,\psi))^m$.

First, let $f(x) = x^d - c_1 x^{d-1} + c_2 x^{d-2} + \cdots + (-1)^d c_d \in \mathbb{F}_q[x]$ and set $\lambda(f) = \chi(c_d)\psi(c_1)$. We define the function

$$L(t,\lambda) = \sum_{f \in \mathbb{F}_q[x] \text{ monic}} \lambda(f) t^{\deg(f)} \ .$$

The claim is that $L(t,\lambda) = 1 + g(\chi,\psi)t$. It is clear that the first term is 1. When $\deg(f) = 1$ and f is monic, $f(x)$ is of the form $x - c_1$. Thus $c_1 = c_d$, and so $\lambda(f) = \chi(c_1)\psi(c_1)$. Now as the sum runs over all monic polynomials of degree 1, each element in $\mathbb{F}_q$ appears only once, so the first two terms of $L(t,\lambda)$ are

$$1 + \sum_{c \in \mathbb{F}_q} \chi(c)\psi(c)t = 1 + g(\chi,\psi)t \ .$$

To prove the claim, we need only prove that, for $d \geq 2$,

$$\sum_{\substack{f \in \mathbb{F}_q[x] \text{ monic} \\ \deg f = d}} \lambda(f) = 0$$

Since $\lambda(f)$ depends only on two of the coefficients of f, we get

$$\sum_{\substack{f \in \mathbb{F}_q \text{ monic} \\ \deg f = d}} \lambda(f) = \sum_{c_1, c_2, \ldots, c_d \in \mathbb{F}_q} \chi(c_d)\psi(c_1) = q^{d-2} \sum_{c_1, c_d \in \mathbb{F}_q} \chi(c_d)\psi(c_1) \ .$$

Since c_1, c_d both range over all of $\mathbb{F}_q$, this final sum is equal to

$$q^{d-2} \big(\sum_{c_1 \in \mathbb{F}_q} \psi(c_1) \big) \big(\sum_{c_d \in \mathbb{F}_q} \chi(c_d) \big) \ .$$

Both of these sums is zero, so we are done. For instance, $\sum \chi(c_d)$ is just the sum over all the n^{th} roots of unity — $n \mid q-1$ — multiplied by some constant, which is zero. This proves the claim that $L(t,\lambda) = 1 + g(\chi,\psi)t$.

Now it is easy to show that $\lambda(fg) = \lambda(f)\lambda(g)$, so factoring the monic polynomials $f(x) \in \mathbb{F}_q[x]$ into irreducible factors and noting that every polynomial is uniquely determined by its irreducible factors, we get

$$L(t,\lambda) = \prod_{\substack{p(x) \in \mathbb{F}_q[x] \\ \text{monic, irreducible}}} (1 - \lambda(p) t^{\deg(p)})^{-1}$$

using a geometric series expansion. Taking the logarithmic derivative of $L(t,\lambda)$ with respect to t yields

$$\frac{L'}{L} = \sum_{\substack{p(x) \in \mathbb{F}_q[x] \\ \text{monic} \\ \text{irreducible}}} \frac{\lambda(p) \deg(p) t^{\deg(p)-1}}{1 - \lambda(p) t^{\deg(p)}} = \sum_{m=1}^{\infty} \big(\sum_{\substack{p(x) \in \mathbb{F}_q[x] \\ \deg(p) \mid m}} \deg(p) \lambda(p)^{m/\deg(p)} \big) t^{m-1}$$

repeating a previous calculation by expanding in a geometric series and then grouping polynomials by degree. We previously established that if $\alpha \in \mathbb{F}_{q^m}$ has minimal polynomial

$p(x)$ with $\deg(p) = d$ dividing m, then $\lambda(p)^{m/d} = \psi_m(\alpha)\chi_m(\alpha)$. Let $\alpha_1, \ldots, \alpha_d$ be the Galois conjugates of α; then

$$\deg(p)\lambda(p)^{m/d} = \sum_{i=1}^{d} \psi_m(\alpha_i)\chi_m(\alpha_i)$$

because $\lambda(p)^{m/d}$ is the same regardless of which root is used to calculate $\psi_m(\alpha_i)\chi_m(\alpha_i)$. Now we have a bijection between Galois orbits of size d and irreducible polynomials of degree $d \mid m$. Going back to our sum, if $d = \deg(p)$, then

$$\sum_{d|m} d\lambda(p)^{m/d} = \sum_{\alpha \in \mathbb{F}_{q^m}} \psi_m(\alpha)\chi_m(\alpha) = g(\chi_m, \psi_m) \ .$$

But $L'/L = \frac{g(\chi,\psi)}{1+g(\chi,\psi)t} = \sum_{m=1}^{\infty}(-1)^{m-1}g(\chi,\psi)^m t^{m-1}$ when we expand in a geometric series. Comparing terms shows that

$$(-1)^{m-1}g(\chi,\psi)^m = g(\chi_m, \psi_m)$$

which proves the Hasse-Davenport formula after multiplication by -1.

Exercise 6.1. Express the zeta function of $y^p - y = x^m$ over $\mathbb{F}_q$ where $q = p^n \equiv 1 \pmod{m}$ as a product of L-functions $L(t, \lambda)$.

We will now prove the Riemann Hypothesis for this function. It is equivalent to the following formula.

Theorem 6.2. $|g(\chi, \psi)| = \sqrt{q}$.

Proof. First recall that $g(\chi,\psi) = \sum_{x \in \mathbb{F}_q^*} \chi(x)\psi(x)$. Thus if we take the absolute value of $g(\chi,\psi)$ and square it, we get

$$|g(\chi,\psi)|^2 = \big(\sum_{x \in \mathbb{F}_q^*} \chi(x)\psi(x)\big)\big(\sum_{y \in \mathbb{F}_q^*} \overline{\chi(y)\psi(y)}\big) = \sum_{x,y \in \mathbb{F}_q^*} \chi(x)\psi(x)\overline{\chi(y)\psi(y)} \ .$$

Since every element in the image of either χ or ψ is a root of unity and roots of unity have absolute value 1, we can conclude that $\overline{\chi(y)} = \chi(y^{-1})$ and $\overline{\psi(y)} = \psi(-y)$. Now replace x by ty, and our sum becomes

$$\sum_{t,y \in \mathbb{F}_q^*} \chi(ty)\psi(ty)\chi(y^{-1})\psi(-y) = \sum_{t,y \in \mathbb{F}_q^*} \chi(t)\psi((t-1)y)$$

which we can then separate out into the sum

$$\sum_{t \in \mathbb{F}_q^*} \chi(t) \sum_{y \in \mathbb{F}_q^*} \psi((t-1)y) \ .$$

First consider the sum $\sum_{y \in \mathbb{F}_q} \psi((t-1)y)$. When $t = 1$, we have

$$\sum_{y \in \mathbb{F}_q} \psi(0) = q\psi(0) = q$$

since $\psi(0) = 1$. When $t \neq 0$, this sum ranges over all the elements in $\mathbb{F}_q$ and thus is equal to zero. Therefore

$$\begin{aligned}\sum_{t\in\mathbb{F}_q^*} \chi(t)\big(\sum_{y\in\mathbb{F}_q^*} \psi((t-1)y)\big) &= \sum_{t\in\mathbb{F}_q^*} \chi(t)\big(-1+\sum_{y\in\mathbb{F}_q} \psi((t-1)y)\big) \\ &= q-1+\sum_{t\neq 0,1} \chi(t)\big(-1+\sum_{y\in\mathbb{F}_q} \psi((t-1)y)\big) \\ &= q-1-\sum_{t\neq 0,1} \chi(t) \\ &= q-1-\sum_{t\in\mathbb{F}_q} \chi(t)+\chi(1) = q\ ,\end{aligned}$$

which completes the proof. □

Our discussion so far has been concerned with a smooth affine curve X with coordinate ring R. We defined

$$Z_{X/\mathbb{F}_q}(t) = \exp\Big(\sum_{r=1}^{\infty} \#X(\mathbb{F}_{q^r})\frac{t^r}{r}\Big)$$

and

$$\zeta_R(s) = \sum_{\substack{I\neq(0)\\ \text{ideal in } R}} \frac{1}{(NI)^s} = \prod_{\substack{P\neq(0)\\ \text{prime ideal in } R}} \Big(1-\frac{1}{(NP)^s}\Big)^{-1}$$

and proved that $\zeta_R(s) = Z_{X/\mathbb{F}_q}(q^{-s})$. Now let $X = \overline{X} \cap \mathbb{A}^n$ where $\overline{X} \subset \mathbb{P}^n$ is a smooth projective curve. Let $T = \overline{X} \setminus X = \overline{X} \cap H$ where H is the hyperplane at infinity, $H = \mathbb{P}^n \setminus \mathbb{A}^n$. Then T is a finite set of points, and we define $T = T_1 \cup \cdots \cup T_k$ where each T_i is $\mathbb{F}_q$-irreducible and hence a $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$-orbit of points. Define d_i to be the number of points in the set T_i. Thus the zeta function for each of these sets is

$$Z_{T_i/\mathbb{F}_q}(t) = \exp\Big(\sum_{r=1}^{\infty} \#T_i(\mathbb{F}_{q^r})\frac{t^r}{r}\Big)\ .$$

Now if d_i divides r, then the points in T_i have coordinates in $\mathbb{F}_{q^r}$ and so $d_i = \#T_i(\mathbb{F}_{q^r})$. Otherwise, this value is zero. Hence,

$$Z_{T_i/\mathbb{F}_q}(t) = \frac{1}{1-t^{d_i}}\ .$$

This then proves the following formula:

$$Z_{\overline{X}/\mathbb{F}_q}(t) = \Big(\prod_{i=1}^{k} \frac{1}{1-t^{d_i}}\Big) Z_{X/\mathbb{F}_q}(t)\ .$$

We have seen before how

$$\prod_{\substack{P\neq 0\\ \text{prime ideal in } R}} \Big(1-\frac{1}{(NP)^s}\Big)^{-1} = \prod (1-t^{\deg(P)})^{-1}$$

where $t = q^{-s}$; note the similarities between this formula and the one above for $Z_{T_i/\mathbb{F}_q}(t)$.

Define a *prime divisor* of $\overline{X}$ to be a $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$-orbit of points of $\overline{X}$. Thus a prime divisor corresponds to either a prime ideal of R or to one of the sets T_i above. If P is a prime divisor, we define $\deg(P)$ to be the number of points in the orbit of P. Hence we have that the equation (6) above gives

$$Z_{\overline{X}/\mathbb{F}_q}(t) = \prod_{P \text{ prime divisor of } \overline{X}} (1 - t^{\deg(P)})^{-1} \ .$$

A *divisor* of $\overline{X}/\mathbb{F}_q$ is an element of the free abelian group generated by the prime divisors. Thus for any divisor D, we write

$$D = \sum_P n_P P$$

where $n_P \in \mathbb{Z}$ and only a finite number of the n_P are nonzero. We say that a divisor is positive if $n_P \geq 0$ for all prime divisors P. The degree of a general divisor is then defined to be

$$\deg(D) = \sum_P n_P \deg(P) \ .$$

We adopt the following notation from this point. X will denote a smooth projective curve with $X_0 = X \cap \mathbb{A}^n$ an affine piece of X, where X is contained in $\mathbb{P}^n$. R will denote the coordinate ring of X with F its field of fractions. Note that F is the function field of X and is an invariant of the curve that can be computed using any Zariski-open subset. X will always be defined over $\mathbb{F}_q$, and $X(\overline{\mathbb{F}}_q)$ will denote all of the points of X with coordinates in the algebraic closure $\overline{\mathbb{F}}_q$ of $\mathbb{F}_q$. Now $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ acts on $X(\overline{\mathbb{F}}_q)$ and the orbits of this action are the prime divisors P_i with degree defined to be the number of points in this orbit. This is also the degree of the extension obtained by adjoining to $\mathbb{F}_q$ the elements which are the coordinates of the points in the orbit; note of course that $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ fixes $X(\mathbb{F}_q)$. If P_i is a prime divisor corresponding to a prime ideal, we write $\mathfrak{P}_i$ for that ideal.

If $\mathfrak{I}$ is an ideal of R, then it can uniquely be written as a product of prime ideals since R is a Dedekind ring: $\mathfrak{I} = \mathfrak{P}_1^{n_1} \cdots \mathfrak{P}_k^{n_k}$. Thus the divisor corresponding to this ideal is

$$D_{\mathfrak{I}} = \sum_P n_i P_i.$$

Therefore prime ideals of R correspond to irreducible subvarieties of X_0 of zero dimension (that is, a finite set of points) which clearly correspond to an orbit under the Galois action by irreducibility. We define the cardinality of the set $R/\mathfrak{I}$ to be the norm of $\mathfrak{I}$, denoted $N\mathfrak{I}$; it is also equal to $q^{\deg(D_{\mathfrak{I}})}$. Then we have

$$Z_X(t) = \sum_{D \geq 0 \text{ divisor}} t^{\deg(D)} = \prod_{P \text{ prime divisor}} (1 - t^{\deg(P)})^{-1} \ .$$

Using the change of variables $t = q^{-s}$ and the fact that there are only a finite number of prime divisors of each degree and hence only a finite number of divisors of each degree,

our calculations yield

$$\sum_{\substack{\mathfrak{I}\neq 0\\ \text{ideal in } R}} \frac{1}{(N\mathfrak{I})^s} = \sum_{D\geq 0} t^{\deg(D)} = \sum_{d=0}^{\infty} (\#\{D \geq 0 : \deg(D) = d\})t^d \ .$$

Let $f \in R$ and consider the principal ideal $(f) \subset R$. Thus we can write $(f) = \mathfrak{P}_1^{n_1} \cdots \mathfrak{P}_k^{n_k}$. Set n_i equal to $v_{P_i}(f)$, and define $v_P(f) = n$ if $f \in \mathfrak{P}^n \setminus \mathfrak{P}^{n+1}$. Now if $h = f/g$ is an element of F^*, then $v_P(h) = v_P(f) - v_P(g)$. By taking a different affine subset $X_0 \subset X$, we can define v_P for all prime divisors P. As an example, let $X = \mathbb{P}^1$ and $X_0 = \mathbb{A}^1$. Then $R = \mathbb{F}_q[x]$ and the roots of monic irreducible polynomials are the Galois orbits as prime ideals correspond to monic irreducible polynomials. The prime divisor at infinity corresponds to the single point at infinity, which in turn corresponds to the ideal $(\frac{1}{x}) \subset \mathbb{F}_q[\frac{1}{x}]$; thus $v_\infty(f) = -\deg(f)$ for $f \in \mathbb{F}_q[x]$. We will not prove the following theorem, though it will be useful.

Theorem 6.3 (Product Formula)**.** *For all $f \in F^*$, $\sum_P v_P(f)\deg(P) = 0$.*

From the example above using $X = \mathbb{P}^1$, let $f(x) = a(x)/b(x) \in F^*$ with a, b relatively prime. Write $a(x) = \prod p_i^{n_i}$ and $b(x) = \prod q_j^{m_j}$ where the polynomials p_i, q_j are irreducible. We know that $v_P(f) = v_P(a) - v_P(b)$. When P corresponds to p_i, this makes $v_P(f) = n_i$; if P corresponds to q_j, then $v_P(f) = -m_j$. Thus

$$\sum_P v_P(f)\deg(P) = \sum n_i \deg(P_i) - \sum m_j \deg(Q_j) + \deg(b) - \deg(a) = 0$$

since $\deg(a) = \sum n_i \deg(p_i)$ and $\deg(b) = \sum m_j \deg(q_j)$.

To justify the name product formula, set $|f|_P = q^{-v_P(f)}$, then the theorem above is equivalent to

$$\prod_P |f|_P^{\deg(P)} = 1 \ .$$

Now let $f \in F^*$. Then the divisor of f, written (f), is defined to be the divisor $\sum_P v_P(f)P$. The product formula then shows that $\deg(f) = 0$ for all $f \in F^*$. If D_1, D_2 are divisors on X, then we say that D_1 is linearly equivalent to D_2 if there exists some $f \in F^*$ such that $D_1 - D_2 = (f)$; if this is the case, we write $D_1 \sim D_2$. Since $\deg(f) = 0$ for all functions f, it is a necessary condition, for $D_1 \sim D_2$, that D_1 and D_2 have the same degree.

Exercise 6.2. If $X = \mathbb{P}^1$, show that $D_1 \sim D_2$ if and only if $\deg(D_1) = \deg(D_2)$.

Let D be a divisor on X. Then we define the vector space $L(D)$ by

$$L(D) = \{f \in F^* : D + (f) \geq 0, \text{ or equivalently, } (f) \geq -D\} \cup \{0\} \ .$$

Now $L(D)$ is an $\mathbb{F}_q$-vector space and is finite dimension; we let $l(D)$ denote its dimension.

For example, once again let $X = \mathbb{P}^1$ and let $D = n \cdot \infty$. Then $f \in L(D)$ if and only if $v_\infty \geq -n$ and $v_P(f) \geq 0$ for all divisors P that are not the prime divisor at infinity. The first condition requires that the degree of f be at most n, and the second condition is equivalent to saying that f has no poles except at infinity, thus is a polynomial.

Therefore $L(D)$ is the vector space of polynomials of degree at most n and has dimension $l(D) = n + 1$.

We will not prove this next theorem, though it will be used repeatedly and is of great importance.

Theorem 6.4 (Riemann-Roch Theorem)**.** *Let X be a smooth projective curve. Then there exists a divisor K and an integer g (the genus of X) such that for all divisors D of X,*

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

If $\deg(D) < 0$, then $f \in L(D)$ implies that $\deg(f) \geq -\deg(D) > 0$, which is impossible by the product formula. Thus $L(D) = \{0\}$ and $l(D) = 0$. This proves that if $\deg(D) > \deg(K)$, then $l(K - D) = 0$. Hence for sufficiently large n, the example above and these remarks show that the genus of $\mathbb{P}^1$ is zero. We now claim that $l(0) = 1$ and $L(0) = \mathbb{F}_q$. If $f \in L(0)$, then $(f) \geq 0$ and so $v_P(f) \geq 0$ for all prime divisors P. This implies that f has no poles, and is therefore a constant. Therefore $f \in \mathbb{F}_q$, proving the claim.

Now when $D = 0$,

$$1 = l(0) = \deg(0) + 1 - g + l(K)$$

proving that $l(K) = g$. If $D = K$, then

$$g = l(K) = \deg(K) + 1 - g + l(0) = \deg(K) + 2 - g \ .$$

This shows that $\deg(K) = 2g - 2$. Note that K is not a uniquely determined divisor, though — it is determined only up to linear equivalence.

7. Week Seven

Example 7.1. Suppose $\operatorname{char} \mathbb{F}_q \neq 2$. Consider the elliptic curve $X : y^2 = f(x)$ where $f(x)$ is a cubic polynomial with no repeated roots. Let O denote the unique point at infinity. A function z on X can be written as $z = a + by$, where a and b are rational functions in x. If z has no affine poles then clearly neither does $\bar{z} = a - by$, since the automorphism $(x, y) \mapsto (x, -y)$ will interchange poles of z and $\bar{z}$. It follows that $a = (z + \bar{z})/2$ has no poles, hence is a polynomial. With a bit more effort we can also show that b is a polynomial in this case. One can also show that x has a double pole at O while y has a triple pole at O. Thus the elements of $L(nO)$ are of the form $a + by$, with $\deg a \leq n/2, \deg b \leq (n - 3)/2$. Hence $l(nO) = n$ so, by Riemann-Roch, the genus of X is 1.

Example 7.2. For a smooth plane curve of degree d, the genus is $\frac{(d-1)(d-2)}{2}$. Hence if $d = 3$, the genus is 1. This can be shown as follows. If H is the divisor cut on the curve by the line at infinity then $x, y \in L(H)$, so $x^i y^j \in L(nH)$ if $i + j \leq n$. Using the smoothness of the curve, it can be shown that these monomials generate $L(nH)$ and the relations are generated by those of the form $x^i y^j f(x, y) = 0, i + j \leq n - d$, where $f(x, y) = 0$ is the equation of the curve. Hence $l(nH) = \binom{n+2}{2} - \binom{n-d+2}{2} = nd - d(d - 3)/2$. As before, Riemann-Roch gives us the genus.

Let $\operatorname{Div} X$ denote the group of divisors of X, that is the free abelian group generated by the prime divisors of X. Recall that we defined a degree map $\deg : \operatorname{Div} X \to \mathbb{Z}$ which is clearly a homomorphism. Let $\operatorname{Div}_0 X$ be the kernel of this map, i.e., the subgroup of divisors of degree zero. Let $\delta > 0$ be such that $\deg(\operatorname{Div} X) = \delta\mathbb{Z}$ (for curves over finite fields, we will show below that $\delta = 1$). We defined above, for every $f \in F^*$ a divisor (f) such that $\deg(f) = 0$ (by the product formula). We have an exact sequence

$$F^* \longrightarrow \operatorname{Div}_0 F \longrightarrow \operatorname{Pic}_0 X \longrightarrow 0$$

where $\operatorname{Pic}_0 X$ is the class group of X (or F). Let H_∞ be the subgroup of $\operatorname{Pic}_0 X$ generated by the divisors at infinity. If there is a divisor of degree one supported at infinity then the class group $\operatorname{Cl}(R) \simeq \operatorname{Pic}_0 X / H_\infty$.

Theorem 7.3. *If X is a curve defined over a finite field then $\operatorname{Pic}_0 X$ is finite and, denoting $h = \#\operatorname{Pic}_0 X$, the number of divisor classes of degree d for any d in $\delta\mathbb{Z}$ is also h.*

Proof. There exist only finitely many prime divisors of any degree since they correspond to orbits points defined over a fixed finite field. Hence there are only finitely many positive divisors of a given degree. We have that $\deg K = 2g - 2 = \delta m$ for some $m \in \mathbf{Z}$. Let $D_1, \ldots, D_h$ be a maximal set of inequivalent positive divisors of degree $\delta(m+1)$, which we know is finite. We proceed to show that for any d in $\delta\mathbb{Z}$ there are exacly h classes of divisors of degree d. Let D_0 be a divisor of degree δ. Suppose D is a divisor of degree $d = r\delta$. Consider the divisor $D' = D + (m+1-r)D_0$ which has degree $(m+1)\delta$. So, $\deg(K - D') < 0$ and therefore $l(K - D') = 0$. The Riemann-Roch theorem then gives $l(D') = \deg D' + 1 - g > 0$. So there exists $f \in L(D') \setminus \{0\}$, i.e., $(f) + D' \geq 0$. But $(f) + D'$ has degree $(m+1)\delta$. So $(f) + D' \sim D_i$ for some $i \in \{1, \ldots, h\}$. Therefore, $D \sim D_i - (m+1-r)D_0$ for some i. For fixed r, the $D_i - (m+1-r)D_0$ are all inequivalent, since the D_i are inequivalent, and this shows that there are exacly h classes of divisors of degree d. □

Example 7.4. For elliptic curves, $\delta = 1$. Every divisor of degree r is equivalent to $D_i - (1-r)O$ for some i. Here the D_i are positive divisors of degree one, so are rational points. One can show that the correspondence $X(\mathbb{F}_q) \to \operatorname{Pic}_0(X) : P \mapsto P - O$ is an isomorphism of groups, where $X(\mathbb{F}_q)$ has the group structure given by the familiar chord and tangent process.

Remark 7.5. The notions of prime divisor, Pic_0, etc.,depend on the choice of the finite field. For all $n \geq 1$, we can consider $\operatorname{Pic}_0(X/\mathbb{F}_{q^n})$. One can show that there exists an algebraic variety J_X over $\mathbb{F}_q$ of dimension g called the Jacobian of X, which is an algebraic group and satisfies $J_X(\mathbb{F}_{q^n}) = \operatorname{Pic}_0(X/\mathbb{F}_{q^n})$ for all $n \geq 1$.

Returning to zeta functions, recall

$$Z_X(t) = \sum_{D \geq 0} t^{\deg D} = \sum_{d=0}^{\infty} \#\{D \geq 0 : \deg D = d\} t^d \ .$$

Note that if $d = r\delta$,

$$\#\{D \geq 0 : \deg D = d\} = \sum_{i=1}^{h} \#\{D \geq 0 : D \sim D_i - (m+1-r)D_0\} \ .$$

Lemma 7.6. *If $r \geq m+1$, then*

$$\#\{D \geq 0 : D \sim D_i - (m+1-r)D_0\} = \frac{q^{r\delta+1-g}-1}{q-1} \ .$$

Proof. An element of the set $\{D \geq 0 : D \sim D_i - (m+1-r)D_0\}$ is of the form

$$D = (f) + D_i - (m+1-r)D_0$$

for some $f \in L(D_i - (m+1-r)D_0)$, with $f \neq 0$. Two functions f_1, f_2 give the same divisor if and only if $f_1 = \lambda f_2$ for some $\lambda \in \mathbb{F}_q^*$. By Riemann-Roch,

$$\dim_{\mathbb{F}_q} L(D_i - (m+1-r)D_0) = r\delta + 1 - g$$

if $r\delta > 2g-2$. Then

$$\#L(D_i - (m+1-r)D_0) = q^{r\delta+1-g} \ .$$

Now noting $\#\mathbb{F}_q^* = q-1$ gives the lemma. □

Let X be a smooth projective curve of genus g over $\mathbb{F}_q$. For some $\delta > 0$, $\deg(\operatorname{Div} X) = \delta\mathbf{Z}$, with $2g-2 = m\delta$. The class number

$$h = \#\{D \in \operatorname{Div} X : \deg D = 0\}/\{(f) : f \in F^*\}$$

where F is the function field of X. We showed $\forall d \in \delta\mathbf{Z}$, the number of divisor classes of degree d is also h. If D has degree $d = r\delta > 2g-2$, then

$$\#\{D' \geq 0 : D' \sim D\} = \frac{q^{r\delta+1-g}-1}{q-1} \ .$$

Hence for the zeta function $Z_X(t) = \sum_{d=0}^{\infty} a_d t^d$,

$$a_d = h\frac{q^{r\delta+1-g}-1}{q-1}$$

if $d = r\delta > 2g-2$. We write

$$\begin{aligned} Z_X(t) &= \sum_{d=0}^{2g-2} a_d t^d + \sum_{r=m+1}^{\infty} h\frac{q^{r\delta+1-g}-1}{q-1}t^{r\delta} \\ &= \sum_{d=0}^{2g-2} a_d t^d + \frac{h}{q-1}\left(q^{1-g}\frac{(qt)^{(m+1)\delta}}{1-(qt)^{\delta}} - \frac{t^{(m+1)\delta}}{1-t^{\delta}}\right) \end{aligned}$$

This proves the following

Theorem 7.7. *For a curve X over a finite field the zeta function $Z_X(t) \in \mathbf{Q}(t)$.*

We also notice that the above formula shows that $Z_X(t)$ has simple poles at α when $\alpha^\delta = 1$. In particular, $Z_X(t)$ has a simple pole at $\alpha = 1$.

We would like to prove that $\delta = 1$. If we could prove that there exists a prime divisor P_n of degree n, for any $n \geq n_0$, then we could show $\delta = 1$ by considering $P_n - P_{n-1}$. We will not proceed this way; our proof will be analytic.

Lemma 7.8.

$$Z_{X/\mathbb{F}_{q^k}}(t^k) = \prod_{\zeta^k=1} Z_{X/\mathbb{F}_q}(\zeta t) \ .$$

Proof. Note

$$Z_{X/\mathbb{F}_q}(t) = \exp\Big(\sum_{n=1}^{\infty} \#X(\mathbb{F}_{q^n})\frac{t^n}{n}\Big) \ .$$

The right side in the statement of the lemma is

$$\begin{aligned}\prod_{\zeta^k=1} Z_{X/\mathbb{F}_q}(\zeta t) &= \exp\Big(\sum_{n=1}^{\infty} \#X(\mathbb{F}^{q^n})\Big(\sum_{\zeta^k=1}\zeta^n\Big)\frac{t^n}{n}\Big) \\ &= \exp\sum_{r=1}^{\infty} \#X(\mathbb{F}_{q^{kr}})k\frac{t^{kr}}{kr}\end{aligned}$$

which equals the left side. □

This proof works for any algebraic variety over $\mathbb{F}_q$.

Theorem 7.9. $\delta = 1$.

Proof. Apply the lemma with $k = \delta$.

$$Z_{X/\mathbb{F}_{q^\delta}}(t^\delta) = \prod_{\alpha^\delta=1} Z_{X/\mathbb{F}_q}(\alpha t) \ .$$

We check on both sides for poles at $t = 1$. Since $Z_{X/\mathbb{F}_q}(t)$ has a pole at $\alpha, \alpha^\delta = 1$, $Z_{X/\mathbb{F}_q}(\alpha t)$ has a pole at $t = 1$. So the right side has a pole of order δ at $t = 1$. We know from above that $Z_{X/\mathbb{F}_{q^\delta}}(t)$ has a simple pole at $t = 1$ and this implies that $Z_{X/\mathbb{F}_{q^\delta}}(t^\delta)$ has a simple pole at $t = 1$. Therefore, $\delta = 1$. □

Corollary 7.10. *An elliptic curve over a finite field is non-empty.*

Proof. Since $\delta = 1$, there exists a divisor of degree 1, say D. Then $L(D)$ has dimension

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

there exists $f \neq 0$, $(f) + D \geq 0$. Now, $(f) + D$ is a poistive divisor of degree one, that is, a rational point. □

Remark 7.11. This is not true for higher genus.

Exercise 7.1. (This is an open problem) Determine all pairs (g, q) for which there exists $X/\mathbb{F}_q$ of genus g with $X(\mathbb{F}_q) = \emptyset$.

For any curve,

$$Z_X(t) = \frac{P(t)}{(1-t)(1-qt)}$$

with $P(t) \in \mathbb{Z}[t]$ and $\deg(P) \leq 2g$. In fact,

$$P(t) = (1-t)(1-qt)(\sum_{d=0}^{2g-2} a_d t^d) + \frac{h}{q-1}(q^{1-g}(1-t)(qt)^{2g-1} - (1-qt)t^{2g-1}).$$

From the definition of the zeta function we see that $P(0) = Z_X(0) = 1$ and by the above formula, $P(1) = h$. This is known as the class number formula.

The leading coefficient of $P(t)$ is

$$qa_{2g-2} + \frac{h}{q-1}(q - q^g)$$

and

$$a_{2g-2} = \#\{D \geq 0 : \deg(D) = 2g-2\} = \sum_{i=1}^{h} \#\{D \geq 0 : D \sim E_i\}$$

where $E_1, \ldots, E_h$ are representatives of the distinct divisor classes of degree $2g-2$. This number is also

$$\sum_{i=1}^{h} \frac{q^{l(E_i)} - 1}{q-1}$$

By Riemann-Roch,

$$l(E_i) = 2g - 2 + 1 - g + l(K - E_i) = g - 1 + l(K - E_i)$$

Lemma 7.12. *If $E_i \sim K$ then $l(K - E_i) = 1$. Otherwise, $l(K - E_i) = 0$.*

Proof. If $K \sim E_i$, then $l(K - E_i) = l(0) = 1$. In any case, $l(K - E_i) \geq 0$. If $l(K - E_i) > 0$, then for some $f \neq 0$, $(f) + K - E_i \geq 0$ and has degree zero, so that $(f) + K - E_i = 0$. i.e., $K \sim E_i$. □

It follows from this lemma that $a_{2g-2} = (h-1)(q^{g-1}-1)/(q-1) + (q^g - 1)/(q-1)$ and therefore the leading coefficient of $P(t)$ is q^g.

8. Week Eight

Let $X/\mathbb{F}_q$ be a smooth projective curve of genus g. We have proved last time that:

$$Z_{X/\mathbb{F}_q}(t) = \frac{P(t)}{(1-t)(1-qt)} \ ,$$

where $P(t) = \sum_{i=0}^{2g} b_i t^i$ with $b_0 = 1$ and $b_{2g} = q^g$.

Lemma 8.1. *There exists an integer k and $C > 0$ such that for every $n \geq 1$,*

$$|\#X(\mathbb{F}_{q^{nk}}) - q^{nk}| \leq Cq^{nk/2} \ .$$

We will prove this lemma later, but will use it now.
We can write $P(t) = \prod_{i=1}^{2g}(1-\alpha_i t)$, then:

$$\#X(\mathbb{F}_{q^n}) = q^n + 1 - \sum_{i=1}^{2g} \alpha_i^n \ .$$

Using the lemma, we see that for every $n \geq 1$,

$$\Big|1 - \sum_{i=1}^{2g} \alpha_i^{kn}\Big| \leq Cq^{nk/2} \ ,$$

for the appropriate k and C. Then:

$$\Big|\sum_{i=1}^{2g} \alpha_i^{kn}\Big| \leq (C+1)q^{nk/2} \ .$$

Claim 8.2. *$|\alpha_i| \leq q^{1/2}$, for every $1 \leq i \leq 2g$.*

Proof. Consider:

$$\sum_{i=1}^{2g} \frac{1}{1-\alpha_i^k t} = \sum_{i=1}^{2g}\sum_{n=0}^{\infty} \alpha_i^{kn} t^n = \sum_{n=0}^{\infty} \Big(\sum_{i=1}^{2g} \alpha_i^{kn}\Big) t^n.$$

The series on the right hand side converges if $|t| < q^{-k/2}$. Using the left hand side, this implies that $|\alpha_i^{-k}| \geq q^{-k/2}$, therefore $|\alpha_i| \leq q^{1/2}$. This finishes the proof of the claim. □

Hence, for all $n \geq 1$, we have:

$$|\#X(\mathbb{F}_{q^n}) - q^n - 1| \leq 2gq^{n/2},$$

i.e. we improved the lemma.

Example 8.3. (Elliptic Curves) Let $g = 1$, then:

$$P(t) = 1 - at + qt^2 = (1-\alpha t)(1-\beta t) \ ,$$

for some a, where $\alpha + \beta = a$, $\alpha\beta = q$, and:

$$\#X(\mathbb{F}_{q^n}) = q^n + 1 - \alpha^n - \beta^n \ ,$$

hence:

$$\#X(\mathbb{F}_q) = q + 1 - \alpha - \beta = q + 1 - a \ ,$$

so we would need to find a in order to determine $\#X(\mathbb{F}_q)$.

In general, $P(t) = \prod_{i=1}^{2g}(1-\alpha_i t)$, so $\prod_{i=1}^{2g} \alpha_i = q^g$, i.e. $\prod_{i=1}^{2g}|\alpha_i| = q^g$. Now we also know that $|\alpha_i| \leq q^{1/2}$. Hence, in case $X/\mathbb{F}_q$ is a smooth projective curve of genus g, we must have:

Theorem 8.4. *(Riemann Hypothesis) $|\alpha_i| = q^{1/2}$ for all $1 \leq i \leq 2g$.*

Claim 8.5. $\{q/\alpha_1, \ldots, q/\alpha_{2g}\} = \{\alpha_1, \ldots, \alpha_{2g}\}$.

Proof. We know that for each $1 \leq i \leq 2g$, $\alpha_i\overline{\alpha_i} = |\alpha_i|^2 = q$. On the other hand, $P(t) \in \mathbb{R}[t]$, so $\overline{\alpha_i}$ is also a root of $P(t)$, since α_i is, for each $1 \leq i \leq 2g$. But $\overline{\alpha_i} = q/\alpha_i$. The conclusion follows. □

It follows from the above claim that:

Corollary 8.6 (Functional Equation)**.** $Z_X(\frac{1}{qt}) = q^{1-g}t^{2-2g}Z_X(t)$.

The above argument is not the usual proof of the functional equation. The usual proof of the functional equation proceeds by relating the coefficient a_d to the coefficient a_{2g-2-d}, using the Riemann-Roch theorem, in the formula

$$Z_X(t) = \sum_{d=0}^{2g-2} a_d t^d + \frac{h}{q-1}\Big(q^{1-g}\frac{(qt)^{2g-1}}{1-qt} - \frac{t^{2g-1}}{1-t}\Big) \ ,$$

proved previously.

We will now briefly step aside, and talk about Riemann-Roch theorem in the case of a number field. Recall that if F is a function field, and $f \in F^\times$, then degree of the corresponding divisor (f) is given by the so called *product formula*:

$$\deg(f) = \sum_{\wp} v_\wp(f)\deg(\wp) = 0 \ ,$$

where the sum is taken over all prime divisors $\wp$, and $v_\wp(f) = n$ if $f \in P^n \backslash P^{n+1}$ for the prime ideal P corresponding to $\wp$. The analog of this product formula for the field of rational numbers $\mathbb{Q}$ will be:

$$\sum_p v_p(a)\log p = \log|a| \ ,$$

where the sum is taken over all prime numbers p in $\mathbb{Z}$, for all $a = \pm\prod_p p^{\alpha_p} \in \mathbb{Q}$, $\alpha_p = v_p(a)$. Now suppose K is a number field, i.e. $K/\mathbb{Q}$ is a finite field extension, and let $\alpha \in K^*$. If N is the norm, then the product formula reads:

$$\sum_{\wp} c_\wp v_\wp(\alpha)\log N\wp = \sum_{\sigma: K\hookrightarrow\mathbb{C}} \log|\sigma(\alpha)|] \ ,$$

and then we can consider divisors which are formal sums

$$D = \sum_{\wp} n_\wp \wp + \sum_{\sigma} n_\sigma \sigma \ ,$$

with the $n_\wp$ integers and the n_σ real numbers, and:

$$L(D) = \{\alpha \in K^* : (\alpha) + D \geq 0\} \cup \{0\} \ .$$

Getting back to our business with $X/\mathbb{F}_q$ being a smooth projective curve, we recall that we have:

$$\#X(\mathbb{F}_{q^n}) = q^n + 1 - \sum_{i=1}^{2g} \alpha_i^n \quad \Rightarrow \quad |\#X(\mathbb{F}_{q^n}) - (q^n+1)| \leq 2gq^{n/2} \ .$$

Goppa discovered that one could make good codes out of curves with many points. One of the fundamental questions to be asked in these regards is how large can the number of points get if q is fixed and g varies?

Example 8.7. Let $q = 2$, $n = 1$, then by our result above:

$$|\#X(\mathbb{F}_2) - 3| \leq 2g\sqrt{2} \ .$$

We will now consider some consequences of the above inequality. First we introduce some notation.

Definition 8.8. Define: $N_q(g) = \max\{\#X(\mathbb{F}_q) : X/\mathbb{F}_q \text{ of genus } g\}$, $A_q = \limsup_{g\to\infty} \frac{N_q(g)}{g}$.

Notice that:

$$\#X(\mathbb{F}_q) \leq q + 1 + 2gq^{1/2} \quad \Rightarrow \quad A_q \leq 2\sqrt{q} \ .$$

Serre noticed that the Weil estimate can be improved thus:

Theorem 8.9. $\#X(\mathbb{F}_q) \leq q + 1 + g\big[2q^{1/2}\big]$.

Proof. Notice that $\beta_i = 1 + \big[2q^{1/2}\big] + \alpha_i + \bar{\alpha}_i \in \mathbb{R}$ are algebraic integers for all $1 \leq i \leq g$, and $\sum_{i=1}^g \beta_i, \prod_{i=1}^g \beta_i \in \mathbb{Z}$. Also we have $\alpha_i + \bar{\alpha}_i \geq -2\sqrt{q}$, hence $\alpha_i + \bar{\alpha}_i + 2\sqrt{q} \geq 0$, thus $\beta_i > 0$. Also:

$$\frac{1}{g}\sum_{i=1}^g \beta_i \geq \Big(\prod_{i=1}^g \beta_i\Big)^{1/g} \geq 1 \ ,$$

hence:

$$\sum_{i=1}^g \beta_i \geq g \quad \Rightarrow \quad \sum_{i=1}^g (\alpha_i + \bar{\alpha}_i) \geq -g\big[2q^{1/2}\big] \ ,$$

since $\sum_{i=1}^g \beta_i = g\big(1 + [2q^{1/2}]\big) + \sum_{i=1}^g (\alpha_i + \bar{\alpha}_i)$. Then we obtain:

$$\#X(\mathbb{F}_q) = q + 1 - \sum_{i=1}^g (\alpha_i + \bar{\alpha}_i) \leq q + 1 + g[2q^{1/2}] \ ,$$

hence completing the proof. □

Example 8.10. Let $g = 3$ and $q = 8$, so $X/\mathbb{F}_8$ is a smooth projective curve of genus 3. Then our result implies that:

$$\#X(\mathbb{F}_8) \leq 8 + 1 + 3[2\sqrt{8}] = 24 < 25 = [8 + 1 + 6\sqrt{8}] \ .$$

Next we produce certain bounds on A_q.

Claim 8.11. *We have:*

$$\#X(\mathbb{F}_q) \leq \frac{1}{2}\big\{\sqrt{(8q+1)g^2 + (4q^2 - 4q)g} + (2q + 2 - g)\big\} \ ,$$

and hence:

$$A_q \leq \sqrt{2q}.$$

Proof. Using Riemann Hypothesis, we obtain:

$$\#X(\mathbb{F}_q) \leq \#X(\mathbb{F}_{q^2}) = q^2 + 1 - \sum_{i=1}^{g}(\alpha_i^2 + \overline{\alpha_i}^2) = q^2 + 1 + 2gq - \sum_{i=1}^{g}(\alpha_i + \overline{\alpha_i})^2$$
$$\leq q^2 + 1 + 2gq - \frac{1}{g}\Big(\sum_{i=1}^{g}(\alpha_i + \overline{\alpha_i})\Big)^2 = q^2 + 1 + 2gq - \frac{1}{g}\big(\#X(\mathbb{F}_q) - (q+1)\big)^2.$$

Expressing $\#X(\mathbb{F}_q)$ from above yields (1). To obtain (2), we notice that (1) implies

$$N_q(g) \leq \frac{1}{2}\Big\{\sqrt{(8q+1)g^2 + (4q^2-4q)g} + (2q+2-g)\Big\},$$

then dividing by g and taking lim sup as $g \to \infty$, we obtain:

$$A_q \leq \limsup_{g\to\infty} \frac{1}{2}\left\{\sqrt{(8q+1) + \frac{4q^2-4q}{g}} + \frac{2q+2}{g} - 1\right\}$$
$$= \frac{1}{2}\Big\{\sqrt{8q+1} - 1\Big\} \leq \sqrt{2q},$$

hence proving (2). □

Theorem 8.12 (Drinfeld - Vladut)**.** $A_q \leq \sqrt{q} - 1$.

Proof. We have $\#X(\mathbb{F}_{q^n}) = q^n + 1 - \sum_{i=1}^{g}(\alpha_i^n + \bar{\alpha}_i{}^n)$, where, by Riemann Hypothesis, $\alpha_i = q^{1/2}\omega_i$, with $|\omega_i| = 1$, hence $\omega_i\bar{\omega}_i = 1$. Then:

$$0 \leq \sum_{i=1}^{g}\left|1 + \omega_i + \omega_i^2 + \ldots + \omega_i^k\right|^2 = \sum_{i=1}^{g}\left(\sum_{r=0}^{k}\omega_i^r\right)\left(\sum_{s=0}^{k}\bar{\omega}_i{}^s\right) =$$
$$\sum_{i=1}^{g}\sum_{r,s=0}^{k}\omega_i^r\bar{\omega}_i{}^s = (k+1)g + \sum_{t=1}^{k}(k+1-t)\sum_{i=1}^{g}\left(\omega_i^t + \bar{\omega}_i{}^t\right)$$
$$= (k+1)g + \sum_{t=1}^{k}(k+1-t)\frac{1}{q^{t/2}}\big(q^t + 1 - \#X(\mathbb{F}_{q^t})\big)$$
$$\leq (k+1)g + \sum_{t=1}^{k}(k+1-t)\frac{1}{q^{t/2}}\big(q^t + 1 - \#X(\mathbb{F}_q)\big)\ .$$

This implies:

$$\#X(\mathbb{F}_q) \leq \frac{\Big\{\sum_{t=1}^{k}\frac{(k+1-t)}{q^{t/2}}(q^t+1) + (k+1)g\Big\}}{\Big\{\sum_{t=1}^{k}(k+1-t)q^{-t/2}\Big\}}\ .$$

Dividing both sides of the above inequality by g and letting $g \to \infty$ yields:

$$A_q \leq \frac{k+1}{\sum_{t=1}^{k}(k+1-t)q^{-t/2}} = \Big\{\frac{1}{k+1}\sum_{t=1}^{k}(k+1-t)q^{-t/2}\Big\}^{-1}$$
$$= \Big\{\sum_{t=1}^{k} q^{-t/2} - \frac{1}{k+1}\sum_{t=1}^{k} tq^{-t/2}\Big\}^{-1}$$

then notice that $\sum_{t=1}^{k} tq^{-t/2}$ is convergent as $k \to \infty$, hence $\lim_{k\to\infty} \frac{1}{k+1}\sum_{t=1}^{k} tq^{-t/2} = 0$. Also, $\lim_{k\to\infty}\sum_{t=1}^{k} q^{-t/2} = \frac{1}{q^{1/2}-1}$, hence the result follows. □

There is also a method of Oesterle that, given g and q, extracts the best bound out of the formulas. Let $Oe_q(g)$ be the best such bound. In many cases it is known that $N_q(g) = Oe_q(g)$. There are, however, a few cases where it is known that $N_q(g) < Oe_q(g)$. In these regards, one can ask the following questions.

Exercise 8.1. What is $N_q(g)$?

Exercise 8.2. Is $N_q(g) = Oe_q(g)$ for infinitely many g, given q?

Exercise 8.3. What is A_q?

There is something known in regards to the third question.

Theorem 8.13 (Ihara - Tsfasman - Vladut - Zink)**.** *If q is a square, then:*

$$A_q = \sqrt{q} - 1 \ .$$

Example 8.14. $\frac{2}{9} \leq A_2 \leq \sqrt{2} - 1$.

It has also been proved that there exists $C > 0$ such that $A_q \geq C \log q$, for all q, as well as there exists $B > 0$ such that $A_{p^3} \geq Bp$, when p is prime.

Exercise 8.4. What is the average number of points of a curve of genus g over $\mathbb{F}_q$?

9. Week Nine

We have been using the following fact:

Theorem 9.1. *If $X/\mathbb{F}_q$ is a projective smooth curve, then there exist $d \geq 1, c > 0$ such that*

$$|\#X(\mathbb{F}_{q^{nd}}) - q^{nd}| \leq cq^{nd/2} \quad \forall n \geq 1$$

Now we'll prove it. First we'll prove the upper bound: $\#X(\mathbb{F}_{q^{nd}}) \leq q^{nd} + cq^{nd/2}$

Remark 9.2. Weil gave 2 proofs of RH: one using the Jacobian and one using $X \times X$ which were simplified by Mattuck and Tate and later Grothendieck. In the 1970's, Stepanov introduced an elementary method which led to proofs by Schmidt, Bombieri. We'll present a variant of a proof by Stöhr and Voloch.

Proposition 9.3. *Suppose $X : f(x, y) = 0$ is a plane curve of degree d over $\mathbb{F}_q$ that also satisfies one of the following:*

1. $d < p = \operatorname{char} \mathbb{F}_q$
2. $d^2y/dx^2 \neq 0$
3. *there exists $P \in X$ such that the tangent to X at P has order of contact exactly 2*

then $\#X(\mathbf{F}_q) \leq d(d+q-1)/2$

What does 2 mean? Since we have $f(x,y) = 0$ then $\frac{dy}{dx} = -\frac{\partial f/\partial x}{\partial f/\partial y}$ and $\frac{d^2y}{dx^2} = \frac{d}{dx}(\frac{dy}{dx})$.

A derivation on a field $\mathbf{F}$ is a map $D : \mathbf{F} \to \mathbf{F}$ satisfying:

1. $D(a+b) = Da + Db, \forall a, b \in \mathbf{F}$
2. $D(ab) = aDb + bDa, \forall a, b \in \mathbf{F}$

Once we know dy/dx we can take derivations in $\mathbb{F}_q(x,y)$.

Proof. Let

$$\begin{aligned} F &= (x^q - x)\frac{\partial f}{\partial x} + (y^q - y)\frac{\partial f}{\partial y} \\ &= \frac{\partial f}{\partial y}(y^q - y - \frac{dy}{dx}(x^q - x)) \end{aligned}$$

F vanishes at rational points of X. In fact F vanishes doubly.

$$\begin{aligned} \frac{d}{dx}\big(y^q - y - \frac{dy}{dx}(x^q - x)\big) &= 0 - \frac{dy}{dx} - \frac{dy}{dx}(-1) - \frac{d^2y}{dx^2}(x^q - x) \\ &= -\frac{d^2y}{dx^2}(x^q - x) \end{aligned}$$

vanishes at rational points.

Now $F \not\equiv 0$ since $F' \not\equiv 0$, as that would imply $d^2y/dx^2 \equiv 0$ by the above. We learned that F has double zeroes at the rational points of X and it is not identically zero. Moreover, $\deg F = d + q - 1$. The total number of common zeroes of f and F is at most $d(d+q-1)$ by Bézout. Since rational points are counted twice we get the result. □

Consider $\mathbb{P}^2 \to \mathbb{P}^5$ given by:

$$(x_0 : x_1 : x_2) \to (x_0x_1 : x_0x_2 : x_1x_2 : x_0^2 : x_1^2 : x_2^2)$$

If you have a curve in $\mathbb{P}^2$, you have a curve in $\mathbb{P}^5$. So a curve can be put into many $\mathbb{P}^n$. Isomorphic images should be counted the same.

Suppose $X \subseteq \mathbb{P}^n$. What's the analog of F as above (vanishes at rational points, etc)? Look at $X \cap \mathbb{A}^n$ with coordinates $x_1, \ldots, x_n$. Then

$$(x_1^q - x_1), \ldots, (x_n^q - x_n)$$

have zeroes at rational points. Now choose some function x and X. Define F as follows:

$$F = \begin{vmatrix} (x_1^q - x_1) & (x_2^q - x_1) & \cdots & (x_n^q - x_1) \\ \frac{dx_1}{dx} & \frac{dx_2}{dx} & \cdots & \frac{dx_n}{dx} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{d^{n-1}x_1}{dx^{n-1}} & \frac{d^{n-1}x_2}{dx^{n-1}} & \cdots & \frac{d^{n-1}x_n}{dx^{n-1}} \end{vmatrix}$$

The motivation for the above function are the following considerations. Our initial F is the equation of the tangent line at (x,y) evaluated at (x^q, y^q) which is the image of (x,y)

under the Frobenius map. More generally we consider, for curves in $\mathbb{P}^n$, the equation of the osculating hyperplane to to the curve at a point P evaluated at the Frobenius of P.

Our strategy will be:

1. Show that F vanishes at the rational points of X with multiplicity at least n.
2. Bound total number of zeroes of F by bounding number of poles.
3. Choose the embedding such that $F \not\equiv 0$. (This is not always the case.)
4. Choose the best embedding (We get different bounds for different embeddings.)

The number of poles of F equals $d(q+n) + (2q-2)(1+2+\cdots+(n-1))$ In the most optimistic situation we get

$$\begin{aligned} n\#X(\mathbb{F}_q) &\leq \#(\text{zeroes of F}) \\ &= \#(\text{poles of F}) \\ &\leq d(q+n) + (2q-2)(1+2+\cdots+(n-1)) \end{aligned}$$

Riemann-Roch will allow us to take $d = n+q$. In this case the bound is

$$\begin{aligned} \#X(\mathbb{F}_q) &\leq \big((n+g)(q+n) + (g-1)n(n-1)\big)/n \\ &= q+1+g\Big(\frac{q}{n}+n\Big) \end{aligned}$$

With $n = q^{1/2}$ this gives $\#X(\mathbb{F}_q) \leq q+1+2gq^{1/2}$.

There are a number of things to be worked out first. For instance, in characteristic 2, $\frac{d^2y}{dx^2} \equiv 0$ always!

$$\frac{d^2}{dx^2}\sum a_n x^n = \sum a_n n(n-1)x^{n-2} = 0$$

To get second derivative divide by 2

$$\frac{1}{2}\frac{d^2}{dx^2}\sum a_n x^n = \sum a_n \frac{n(n-1)}{2}x^{n-2}$$

Let k be a field. Define Hasse derivatives (or higher derivatives) $D^{(r)} : k[[x]] \to k[[x]]$ for $r \geq 1$ as follows:

$$D^{(r)}\left(\sum_{n=0}^{\infty} a_n x^n\right) = \sum a_n \binom{n}{r} x^{n-r}$$

We then get:

$$r!D^{(r)} = \frac{d^r}{dx^r}$$

Properties of $D^{(r)}$

1. $D^{(r)}(u+v) = D^{(r)}(u) + D^{(r)}(v)$
2. $D^{(r)}(uv) = \sum_{j=0}^{r} D^{(j)}(u)\, D^{(r-j)}(v)$
3. $D^{(r)}D^{(s)} = \binom{r+s}{r} D^{(r+s)} = D^{(s)}D^{(r)}$

Proof. The first one is obvious.

2) Let $u = \sum a_n x^n, v = \sum b_n x^n$. The coefficient of x^n in uv is $\sum_{i=0}^n a_i b_{n-i}$. The coefficient of x^{n-r} in $D^{(r)}uv$ is $\binom{n}{r}\sum_{i=0}^n a_i b_{n-i}$. The coefficient of x^{n-r} in $D^{(j)}uD^{(r-j)}v$ is $\sum_{l=0}^{n-r}\binom{l+j}{j}a_{l+j}\binom{n-l-j}{r-j}b_{n-l-j}$. The coefficient of x^{n-r} in $\sum_j D^{(j)}uD^{(r-j)}v$ is therefore

$$\sum_{i=0}^{n} a_i b_{n-i} \sum_{j=i-n+r}^{i} \binom{i}{j}\binom{n-i}{r-j} .$$

The inner sum is equal to $\binom{n}{r}$ which gives the result.

Part 3 is similar to part 2. □

Property 2 implies, by induction,

$$D^{(r)}(u_1 \cdots u_j) = \sum_{\substack{s_1+\cdots+s_j=r \\ s_i \geq 0}} D^{(s_1)}(u_1) \cdots D^{(s_j)}(u_j)$$

Lemma 9.4. *If $m, n \in \mathbf{Z}$, $m = \sum m_i p^i, n = \sum n_i p^i, 0 \leq m_i, n_i \leq p-1$, then $\binom{n}{m} \equiv 0 \pmod{p}$ if and only if $m_i \leq n_i, \forall i$.*

Proof. Consider $(1+x)^n \in \mathbb{F}_p[x]$. The coefficient of x^m is $\binom{n}{m}$. On the other hand:

$$\begin{aligned}(1+x)^n = \prod_{i=0}^{d}(1+x)^{n_i p^i} &= \prod_{i=0}^{d}(1+x^{p^i})^{n_i} \\ &= \prod_{i=0}^{d}\left(\sum_{k_i=0}^{b_i}\binom{n_i}{k_i}x^{k_i p^i}\right) \\ = \sum_{0 \leq k_i \leq n_i}\binom{n_0}{k_0}\cdots\binom{n_d}{k_d}&x^{k_0+k_1 p+\cdots+k_d p^d}\end{aligned}$$

We really have proven more: $\binom{n}{m} \equiv \prod_{i=0}^{d}\binom{n_i}{m_i} \pmod{p}$. □

Corollary 9.5. *If $n \equiv 0 \pmod{p^f}$ and $r < p^f$ then $D^{(r)}x^n = 0$ in $\mathbb{F}_p[[x]]$.*

In particular $D^{(r)} \equiv 0$ on $k[[x^{p^f}]]$ if $r < p^f$, $p = \operatorname{char} k > 0$.

Corollary 9.6. *$D^{(r)}$ extends uniquely to $k((x))$.*

Proof. If $p^f > r$ we use,

$$D^{(r)}(\frac{a}{b}) = d^{(r)}(\frac{ab^{p^f-1}}{b^{p^f}}) = \frac{1}{b^{p^f}}D^{(r)}(ab^{p^f-1}) .$$

This proves uniqueness and using equality of both ends gives existence. □

Note that $D^{(r)}$ maps $k[x]$ to itself and, by the proof of the above corollary, it also maps $k(x)$ to itself.

Theorem 9.7. *Suppose $F/k(x)$ is a finite separable extension then $D^{(r)}$ extends uniquely to F (satisfying 1, 2, 3).*

Proof. Assume k is algebraically closed, without loss of generality. We'll prove later that there exists $\alpha \in k$ such that F embeds in $k((x-\alpha))$. Since F is separable $F = k(x,y)$ with $f(x,y) = 0$ and $\frac{\partial f}{\partial y} \not\equiv 0$. Then we can extend $D^{(r)}$ to $k((x-\alpha))$. We note that $D_x^{(r)} = D_{x-\alpha}^{(r)}$ in $k(x)$.

So we get a map $D^{(r)} : k((x-\alpha)) \to k((x-\alpha))$ satisfying 1, 2, and 3, coinciding with the usual $D^{(r)}$ on $k(x)$. What happens to F? We'll prove that $D^{(r)}(F) \subseteq F$. To prove that, it is enough to show that $D^{(r)}(y) \in F$, y defined above.

We will prove more; namely

$$D^{(r)}(y) = \frac{F_r(x,y)}{(\partial f/\partial y)^{2r-1}}$$

where $F_r(x,y) \in k[x,y]$ is uniquely determined by f and r and of degree at most $(2d-3)r - d + 2$ for $r \geq 1$ where $d = \deg f(x,y)$. This will be useful later.

Notation: $\frac{\partial f}{\partial y} = f_y$.

We'll prove the theorem by induction. When $r = 1$:

$$f(x,y) = 0 \Rightarrow f_x + f_y \frac{dy}{dx} = 0$$
$$D^{(1)}y = \frac{dy}{dx} = \frac{-f_x}{f_y}$$

So the formula holds. Now let $r > 1$.

$$0 = f_y^{2r-2} D^{(r)}(f(x,y)) = f_y^{2r-2} D^{(r)} \left(\sum_{i+j \leq d} a_{ij} x^i y^j \right)$$
$$= \sum_{i+j \leq d} a_{ij} \sum_{s=0}^{r} D^{(r-s)} x^i \sum_{s_1 + \cdots + s_j = s} f_y^{2r-2} D^{(s_1)}(y) \ldots D^{(s_j)}(y)$$

Applying the induction hypothesis,

$$0 = \sum_{i+j \leq d} a_{ij} \sum_{s=0}^{r} D^{(r-s)} x^i \sum_{\substack{s_1 + \cdots + s_j = s \\ 0 \leq s_i < r}} f_y^{2r-2} \frac{F_{s_1} \ldots F_{s_j}}{f_y^{2s - \alpha(s_1, \ldots, s_j)}} + f_y^{2d-1} D^{(r)} y$$

with $\alpha(s_1, \ldots s_j) = \#\{i | s_i > 0\}$ and $D^{(0)}y = y = F_0$.

Let

$$F_r = - \sum_{i+j \leq d} a_i j \sum_{s=0}^{r} D^{(r-s)} x^i \sum_{\substack{s_1 + \cdots + s_j = s \\ 0 \leq s_i < r}} f_y^{2r - 2s + \alpha(s_1, \ldots, s_j) - 2} F_{s_1} \ldots F_{s_j} \ .$$

We need to show that F_r is a polynomial in x and y and that $\deg F_r \leq (2d-3)r - d + 2$. It is enough to show that $2r - 2s - 2 + \alpha(s_1, \ldots, s_j) \geq 0$. This is clear if $s < r$. If $s = r$, we want to show $\alpha(s_1, \ldots, s_j) \geq 2$. So when is $\alpha = 0$ or $\alpha = 1$?

$\alpha = 0 \Rightarrow s_i = 0, \forall i \Rightarrow \sum s_i = 0 = s = r$ and we are assuming that $r \geq 1$, which leads to a contradiction, so $\alpha \neq 0$.

$\alpha = 1 \Rightarrow s_i = 0$ for all i such that $i \neq i_0$, so $r = s = \sum s_i = s_{i_0}$, but $r > s_i$, which leads to a contradiction, so $\alpha \neq 1$.

Thus we have proved that F_r is a polynomial.

To estimate the degree of F_r, note that only the terms with $r - s \leq i$ appear in the sum defining F_r, since $D^{(r-s)}x^i = 0$ otherwise. The degree of each such summand is at most

$$\begin{aligned} &i - r + s + (d-1)(2r - 2s + \alpha - 2) + \sum_{s_i > 0} \big((2d-3)s_i - (d-2)\big) + \sum_{s_i = 0} 1 \\ &= i - r + s + (d-1)(2r - 2s + \alpha - 2) + (2d-3)s - (d-2)\alpha + j - \alpha \\ &= (2d-3)r + i + j - 2(d-1) \end{aligned}$$

We note that $i + j \leq d$, so we have proved the bound on the degree. □

10. Week Ten

Lemma 10.1. *Let $f(X, Y)$ be a polynomial with coefficients in a field k. Suppose (x_0, y_0) in k^2 is such that $f(x_0, y_0) = 0$ and $\frac{\partial f}{\partial y}(x_0, y_0) \neq 0$. Then there exists a power series $y = \sum_{i=0}^{\infty} y_i (x - x_0)^i$, with $y_i \in k$, such that $f(x, y) = 0$; i.e., $f(x_0 + (x - x_0), y) = 0$ in $k[[x - x_0]]$.*

Proof. Replacing x by $x - x_0$, we may assume that $x_0 = 0$. We will prove by induction on n that there exist $y_0, y_1, \ldots, y_n$ such that $f(x, y_0 + y_1 x + \cdots + y_n x^n) \equiv 0 \pmod{x^{n+1}}$. If this is true for all n, then

$$y = \sum_{i=0}^{\infty} y_i x^i$$

is such that $f(x, y) = 0$ in $k[[x]]$.

The case $n = 0$ is just the hypothesis, $f(0, y_0) = 0$. Assume the induction hypothesis for n. By assumption, there exists $c \in k$ such that,

$$f(x, y_0 + \cdots + y_n x^n) \equiv c x^{n+1} \pmod{x^{n+2}}. \tag{1}$$

Also,

$$\begin{aligned} f(x, y_0 + y_1 x + \cdots + y_{n+1} x^{n+1}) &\equiv f(x, y_0 + y_1 x + \cdots + y_n x^n) \\ &+ \frac{\partial f}{\partial y}(x, y_0 + y_1 x + \cdots + y_n x^n) y_{n+1} x^{n+1} \pmod{x^{n+2}}. \end{aligned} \tag{2}$$

Combining the above:

$$\begin{aligned} f(x, y_0 + y_1 x + \cdots + y_{n+1} x^{n+1}) &\equiv c x^{n+1} + \frac{\partial f}{\partial y}(x, y_0 + y_1 x + \cdots + y_n x^n) y_{n+1} x^{n+1} \pmod{x^{n+2}} \\ &\equiv c x^{n+1} + \frac{\partial f}{\partial y}(0, y_0) y_{n+1} x^{n+1} \pmod{x^{n+2}} \\ &\equiv (c + \frac{\partial f}{\partial y}(0, y_0) y_{n+1}) x^{n+1} \pmod{x^{n+2}} \end{aligned}$$

So just take

$$y_{n+1} = \frac{-c}{\frac{\partial f}{\partial y}(0, y_0)} \ .$$

□

Lemma 10.2. *Suppose $y \in \mathbb{F}_q[[x]]$. Then*

$$y^q - y = \sum_{r=1}^{\infty} (D^{(r)}y)(x^q - x)^r \ .$$

(Note: $y \in \mathbb{F}_q[[x]]$ implies that the constant coefficient of $y^q - y$ is zero, hence we can start the power series at $r = 1$.)

Remark. The ring of power series has a topology. If

$$y = \sum_{i=0}^{\infty} a_i x^i \text{ and } z = \sum_{i=0}^{\infty} b_i x^i \ ,$$

define $d(y, z) = e^{-n}$ if $a_i = b_i$ for $i < n$ and $a_n \neq b_n$ and $d(y, z) = 0$ if $y = z$. It is trivial to check that this is a metric.

Proof. Note that both sides are continuous functions of y (in the sense of the above metric). Also, both sides are $\mathbb{F}_q$-linear as functions of y. So it is enough to show that the above equality holds for elements in a basis. We take the basis $x^m, m = 0, 1, 2, \ldots$. The left-hand side of the equality, for $y = x^m$, is $x^{qm} - x^m$.

The right-hand side is

$$\begin{aligned} \sum_{r=1}^{\infty} (D^{(r)}x^m)(x^q - x)^r &= \sum_{r=1}^{m} \binom{m}{r} x^{m-r}(x^q - x)^r \\ &= (x^q - x + x)^m - x^m \\ &= x^{qm} - x^m \ . \end{aligned}$$

So we have equality. □

Proposition 10.3. *Suppose $y_1, \ldots, y_n \in \mathbb{F}_q[[x]]$ and let*

$$F = \det \begin{pmatrix} {y_1}^q - y_1 & \cdots & {y_n}^q - y_n \\ Dy_1 & \cdots & Dy_n \\ \vdots & \ddots & \vdots \\ D^{(n-1)}y_1 & \cdots & D^{(n-1)}y_n \end{pmatrix}$$

F has a zero of order at least n at $x = 0$, and the order is exactly n if and only if

$$\Delta = \det \left(D^{(i)}y_j(0)\right)_{i,j=1,\cdots,n} \neq 0 \ .$$

In particular, when $\Delta \neq 0$ we get $F \not\equiv 0$.

Proof. Use the previous lemma. Add to the first row of the matrix defining F the ith row times $-(x^q - x)^i$ for $i = 1, \cdots, n-1$. This obviously will not affect F. Then:

$$F = \det \begin{pmatrix} {y_1}^q - y_1 - \sum_{r=1}^{n-1} (D^{(r)} y_1)(x^q - x)^r & \cdots & {y_n}^q - y_n - \sum_{r=1}^{n-1} (D^{(r)} y_n)(x^q - x)^r \\ Dy_1 & \cdots & Dy_n \\ \vdots & \ddots & \vdots \\ D^{(n-1)} y_1 & \cdots & D^{(n-1)} y_n \end{pmatrix}$$

Now use the lemma, which gives:

$$F = \det \begin{pmatrix} \sum_{r=n}^{\infty} (D^{(r)} y_1)(x^q - x)^r & \cdots & \sum_{r=n}^{\infty} (D^{(r)} y_n)(x^q - x)^r \\ Dy_1 & \cdots & Dy_n \\ \vdots & \ddots & \vdots \\ D^{(n-1)} y_1 & \cdots & D^{(n-1)} y_n \end{pmatrix}$$

All terms in the first row are divisible by x^n, so F is divisible by x^n. We have

$$\begin{aligned} \sum_{r=n}^{\infty} (D^{(r)} y)(x^q - x)^r &\equiv D^{(n)} y (x^q - x)^n \pmod{x^{n+1}} \\ &\equiv D^{(n)} y (-x)^n \pmod{x^{n+1}} \\ &\equiv (D^{(n)} y)(0)(-1)^n x^n \pmod{x^{n+1}} . \end{aligned}$$

Therefore the coefficient of x^n in F is

$$\det \begin{pmatrix} D^{(n)} y_1(0)(-1)^n & \cdots & D^{(n)} y_n(0)(-1)^n \\ Dy_1(0) & \cdots & Dy_n(0) \\ \vdots & \ddots & \vdots \\ D^{(n-1)} y_1(0) & \cdots & D^{(n-1)} y_n(0) \end{pmatrix} = \Delta$$

□

We aim to prove the following:

Theorem 10.4. *Let X be a smooth projective curve over $\mathbb{F}_q$ of genus g. There exist $d \geq 1$ and $C > 0$ such that, for all $m \geq 1$, $\#X(\mathbb{F}_{q^{md}}) \leq q^{md} + Cq^{md/2}$.*

Proof. Let $K = \mathbb{F}_q(X)$ be the function field of X. Choose $x \in K$ such that $K/\mathbb{F}_q(x)$ is finite and separable. Then, by the primitive element theorem, there exists $y \in K$ such that $K = \mathbb{F}_q(x, y)$. So, there exists $f \in F_q[x, y]$ such that $f(x, y) = 0$. Also, $\frac{\partial f}{\partial y} \neq 0$ because this is a separable extension (i.e., we can take f to be the minimal polynomial for y over $F_q[x]$).

Let H be a positive divisor such that all poles of x and y are on the support of H; that is, such that x and y only have poles at points that appear in H. Take d sufficiently large so that there exists $P = (x_0, y_0) \in X(\mathbb{F}_{q^d})$ such that P is not in the support of H and that $\frac{\partial f}{\partial y}(P) \neq 0$. (Since $\frac{\partial f}{\partial y} \not\equiv 0$, this is possible).

Choose $y_1, \cdots, y_n$ in $L(kH)$ for some k as follows. Choose y_i such that $\mathrm{ord}_P(y_i) = i$. (ord_P denotes the order of multiplicity.) To show that this is possible consider

$$L(kH) \supseteq L(kH - P) \supseteq L(kH - 2P) \supseteq L(kH - 3P) \supseteq \cdots$$

Elements in $L(kH - iP)$ have a zero of order at least i at P. So elements in $L(kH - iP) \setminus L(kH - (i+1)P$ have a zero of order exactly i at P. Provided $L(kH - iP) \neq L(kH - (i+1)P)$, we are free to choose y_i.

The Riemann-Roch Theorem yields, for $k \deg H - i > 2g - 1$,

$$l(kH - iP) = k \deg H - i + 1 - g$$

and

$$l(kH - (i+1)P) = k \deg H - i - 1 + 1 - g - i - 1 > 2g - 2 \ .$$

As long as $i < k \deg H - 2g + 1$, we can pick y_i. Now let

$$F_m = \det \begin{pmatrix} {y_1}^{q^{dm}} - y_1 & \cdots & {y_n}^{q^{dm}} - y_n \\ Dy_1 & \cdots & Dy_n \\ \vdots & \ddots & \vdots \\ D^{(n-1)}y_1 & \cdots & D^{(n-1)}y_n \end{pmatrix} \ .$$

Our goal is to get $n = q^{dm/2}$. (Without loss of generality, d is even.) We can reach this value of n if $q^{dm/2} < k \deg H - 2g + 1$. Take k to be the smallest integer satisfying this inequality.

If the y_i's are chosen as above, then $F_m \neq 0$ and $\operatorname{ord}_Q F_m \geq n$ if $Q \in X(\mathbb{F}_{q^{dm}})$ is such that $y_1, \ldots, y_n$ are power series in $x - x(Q)$. We'll prove later that the number of Q's not satisfying this is bounded independently of m, say by some constant C_1. In this event,

$$\#X(\mathbb{F}_{q^{dm}}) \leq C_1 + \deg H + \deg F_m / n \ .$$

Lemma 10.5. *There exists C_2, independent of m, such that for all $r \geq 1$, $D^{(r)}y_i \leq \deg y_i + rC_2$.*

Assuming the lemma, if $y_i \in L(kH)$, then $\deg y_i \leq k \deg H$ and

$$F_m = \sum_\sigma (y_{\sigma(1)}^{q^{md}} - y_{\sigma(1)}) Dy_{\sigma(2)}^{(2)} \cdots Dy_{\sigma(n)}^{(n)}$$

Thus:

$$\begin{aligned} \deg F_m &\leq q^{md}(k \deg H) + k \deg H + C_2 + \cdots + k \deg H + (n-1)C_2 \\ &= (q^{md} + n - 1)k \deg H + \frac{n(n-1)}{2} C_2 \end{aligned}$$

$$\#X(\mathbb{F}_{q^{dm}}) \leq C_1 + \deg H + \frac{1}{n}((q^{md} + n - 1)k \deg H + \frac{n(n-1)}{2} C_2).$$

Recall that k was chosen to be the smallest integer such that $q^{dm/2} < k \deg H + 2g - 1$. Hence $(k-1)\deg H + 2g - 1 \leq q^{dm/2}$. Then $k \deg H = q^{dm/2} + O(1)$. (Remember: $n = q^{dm/2}$.) Therefore

$$\begin{aligned} \#X(\mathbb{F}_{q^{dm}}) &\leq C_1 + \deg H + (q^{md} + n - 1)(1 + O(q^{-md/2})) + \frac{n-1}{2} C_2 \\ &= q^{md} + O(1) + O(q^{md/2}) \ . \end{aligned}$$

□

So all that is left to prove is the lemma:

Proof. Let $y_i \in \mathbb{F}_{q^d}(x,y)$, $f(x,y)=0$. Let δ be the degree in y of $f(x,y)$. Any element y_i can be written

$$y_i = \sum_{j=0}^{\delta-1} a_{ij} y^j, a_{ij} \in \mathbb{F}_{q^d} \ .$$

We need another lemma:

Lemma 10.6. *Suppose $x_0 \in \mathbb{F}_{q^d}$ is such that $f(x_0,y)=0$ has δ distinct roots and that, for each such root y_0, $\frac{\partial f}{\partial y}(x_0,y_0) \neq 0$. Let $z = \sum_{i=0}^{\delta-1} b_i y^i, b_i \in \mathbb{F}_q(x)$ be such that $\operatorname{ord}_{(x_0,y_0)} z \geq 0$ for all y_0 such that $f(x_0,y_0)=0$. Then $ord_{x_0} b_i \geq 0$ for all i.*

Proof. Suppose by way of contradiction that some b_i has a pole at x_0 and let $-r = \min\{\operatorname{ord}_{x_0} b_i\}$, $r>0$. Thus $\operatorname{ord}_{(x_0,y_0)}(x-x_0)^r b_i \geq 0$ for all i. Observe that

$$(x-x_0)^r z = \sum_{i=0}^{\delta-1} (x-x_0)^r b_i y^i \tag{3}$$

vanishes at (x_0,y_0). Let β_i be the value of $(x-x_0)^r b_i$ at $x=x_0$. $\beta_i \in \overline{F}_q$ and not all β_i are 0. The above equation implies that $\sum_{i=0}^{\delta-1} \beta_i {y_0}^i = 0$ for all y_0 satisfying $f(x_0,y_0)=0$. However, $\sum_{i=0}^{\delta-1} \beta_i y^i$ is a nonzero polynomial with degree less than or equal to $\delta-1$, since not all β_i are 0. So it cannot have δ roots, a contradiction. □

We want to show $\deg D^{(r)} y_i \leq \deg y_i + rC_2$. We have

$$\deg D^{(r)} y_i \leq \sum_{j=0}^{\delta-1} D^{(r)} a_{ij} y^j \ .$$

It will be enough to show that

$$\deg D^{(r)} a_{ij} \leq \deg a_{ij} + rC_2$$

and

$$\deg D^{(r)} y \leq \deg y + rC_2 \ .$$

For a rational function a, the order of a pole of $D^{(r)}a$ at $x=x_1$ grows linearly with r. The functions a_{ij} only have poles in the x_j's for which there exists y_1 such that $\frac{\partial f}{\partial y}(x_1,y_1)=0$. So the number of these x_j's is uniformly bounded.

Recall

$$D^{(r)} y = \frac{F_r}{(\frac{\partial f}{\partial y})^{2r-1}}$$

for some $F_r \in \mathbb{F}_q[[x]]$ with $\deg F_r \leq (2\deg f - 3)r - (\deg f - 2)$. So $\deg D^{(r)} y$ grows linearly with r.

□

11. Week Eleven

To complete the Riemann hypothesis for curves, we need to show that given $X/\mathbb{F}_q$, $\exists c > 0, d \geq 1$ such that $\forall n \geq 1$,

$$|\#X(\mathbb{F}_{q^{nd}}) - q^{nd}| \leq cq^{nd/2} \ .$$

We have proved the upper bound $\#X(\mathbb{F}_{q^{nd}}) - q^{nd} \leq cq^{nd/2}$. So now we want to prove the lower bound. We will show that, for a given n, there are curves $X_1, \ldots, X_m$ defined over $\mathbb{F}_{q^n}$, with $X_1 = X$, such that

$$\frac{1}{m}\sum_{i=1}^{m} \#X_i(\mathbb{F}_{q^n}) = q^n + O(q^{\frac{n}{2}}) \ , \tag{4}$$

where the O constant is independent of n. We can apply the upper bound, proved before, to the curves $X_2, \ldots, X_m$, and get

$$\begin{aligned} \#X(\mathbb{F}_{q^{nd}}) &= mq^{nd} - \sum_{i=2}^{m} \#X_i(\mathbb{F}_{q^{nd}}) + O(q^{\frac{nd}{2}}) \\ &\geq mq^{nd} - \sum_{i=2}^{m} (q^{nd} + cq^{\frac{nd}{2}}) + O(q^{\frac{nd}{2}}) = q^{nd} + O(q^{\frac{nd}{2}}) \ . \end{aligned}$$

Observe that the more curves we have, the worse is the constant in the lower bound (it depends on m). Before doing the general case, let's look at an example.

Example 11.1. Let $X_1/\mathbb{F}_q$ be the curve defined by $y^2 = f(x)$, where $f(x) \in \mathbb{F}_q[x]$. Suppose that q is odd. Take $c \in \mathbb{F}_q{}^* \setminus (\mathbb{F}_q{}^*)^2$ ($(\mathbb{F}_q{}^*)^2$ is a subgroup of $\mathbb{F}_q{}^*$ of index 2).

Consider $X_2/\mathbb{F}_q$ defined by $y^2 = cf(x)$. Then we claim that

$$\#X_1(\mathbb{F}_q) + \#X_2(\mathbb{F}_q) = 2(q+1)$$

counting the points at infinity too. To see this, observe that if, $x \in \mathbb{F}_q$ is such that $f(x)$ is a square in $\mathbb{F}_q$, then we get 2 points in X_1 and 0 points in X_2. If, on the other hand, $f(x)$ is not a square in $\mathbb{F}_q$, then we get 0 points in X_1 and 2 points in X_2. Finally, if $f(x) = 0$ then we get 1 point in X_1 and 1 point in X_2. So, adding all those points with the points at infinity of X_1 and X_2, we get $2(q+1)$, as desired.

The example above gives us the oportunity to introduce a new definition:

Definition 11.2. Let X be a curve over a field K. Suppose that Y is another curve defined over K such that X and Y are isomorphic over $\overline{K}$, the algebraic closure of K. Then we call Y a *twist* of X (in the example above, X_2 is a twist of X_1). If X and Y are isomorphic over K, we say that the twist is *trivial*.

Now, suppose that Y is a non-trivial twist of X and assume that K is perfect. Let $\phi : X \to Y$ be an isomorphism over $\overline{K}$. (The coefficients of the expressions that determine ϕ cannot be in K, otherwise the twist would be trivial.)

We can take, for $\sigma \in \mathrm{Gal}(\overline{K}/K)$, the map $\phi^\sigma : X \to Y$ by making σ act on the coefficients of the expressions that define ϕ. So we can consider $\phi^{-1} \circ \phi^\sigma : X \to X$, $\phi^{-1} \circ \phi^\sigma \in \mathrm{Aut}(X)$. Call it ξ_σ.

Observe that $\xi_{\tau\sigma} = \phi^{-1} \circ \phi^\sigma \circ (\phi^{-1})^\sigma \circ \phi^{\tau\sigma} = (\phi^{-1} \circ \phi^\sigma) \circ (\phi^{-1} \circ \phi^\tau)^\sigma = \xi_\sigma {\xi_\tau}^\sigma$. Things like this one are called Galois 1-cocycles with coefficients in $\mathrm{Aut}(X)$.

If $K = \mathbb{F}_q$, it is enough to know the value of ξ_σ when σ is the Frobenius automorphism ($\sigma(x) = x^q$). to determine the whole cocycle, since the Frobenius automorphism generates the Galois group.

Theorem 11.3. *Given $X/\mathbb{F}_q$ and $g \in Aut(X)$ of finite order, there exists a twist $X^{(g)}$ of X which is isomorphic to X over $\mathbb{F}_{q^{ord(g)}}$ and, moreover, for every finite subgroup H of $Aut(X)$,*

$$\frac{1}{|H|}\sum_{h\in H} \#X^{(h)}(\mathbb{F}_q) = \#(X/H)(\mathbb{F}_q) \ .$$

In the proof of the theorem, It will become clear what X/H means. Before proving the theorem, let's see an example.

Example 11.4. Let X be defined by $y^2 = f(x)$, and $g \in \mathrm{Aut}(X)$ given by $g(x, y) = (x, -y)$. Take $H = \{id, g\}$. Then $X/H = \mathbb{P}^1$, $X^{(g)}$ is given by $y^2 = cf(x)$. Take $\phi : X \to X_2$ given by $(x, y) \mapsto (x, \sqrt{c}y)$.

If $\sigma =$ Frobenius, then $\phi^{-1} \circ \phi^\sigma(x, y) = \phi^{-1}(x, -\sqrt{c}y) = (x, -y) = g(x, y)$. Observe that $\phi^\sigma(x, y) = (x, \sigma(\sqrt{c})y) = (x, (\sqrt{c})^q y) = (x, -\sqrt{c}y)$.

Proof. Let L be the function field of X over $\mathbb{F}_q$, $L = \mathbb{F}_q(X)$. Let H be a finite subgroup of $Aut(X)$. So H acts on L. Let $K = L^H$, the fixed field of L by the action of H. So $\mathbb{F}_q \subseteq K \subseteq L$. Since $[L : K]$ is finite, K is not a finite field (since L is not a finite field). So $K/\mathbb{F}_q$ is transcendental and since $K \subseteq L$, K must be finitely generated of transcendence degree 1 over $\mathbb{F}_q$.

So K is the function field of some curve over $\mathbb{F}_q$. That's what we call X/H.

Let $L' = \mathbb{F}_{q^m}(X)$, the function field of X over $\mathbb{F}_{q^m}$, where $m = |H|$. Note that $\mathbb{F}_{q^m} \subseteq L'$, $L \subseteq L'$ and $L' = L\mathbb{F}_{q^m}$.

There is an automorphism σ of L' such that $\sigma|_{\mathbb{F}_{q^m}} =$ Frobenius and $\sigma|_L = \mathrm{id}$.

Define, for $h \in H$, the field $L^{(h)} = (L')^{\langle\sigma\circ h\rangle}$ (we can think of h acting on L' by $h|_{\mathbb{F}_{q^m}} = \mathrm{id}$).

Claim 11.5. *$L^{(h)} \cap \mathbb{F}_{q^m} = \mathbb{F}_q$, $L^{(h)}$ is transcendental over $\mathbb{F}_q$ and $L^{(h)}\mathbb{F}_{q^m} = L'$*

So $L^{(h)}$ is the function field of some curve over $\mathbb{F}_q$. That's what we call $X^{(h)}$ (from $L^{(h)} \cap \mathbb{F}_{q^m} = \mathbb{F}_q$, $L^{(h)}$ transcendental over $\mathbb{F}_q$ and the equivalence between curves and function fields).

From $L^{(h)}\mathbb{F}_{q^m} = L'$ we get that X and $X^{(h)}$ are isomorphic over $\mathbb{F}_{q^m}$.

Proof. $L^{(h)} \cap \mathbb{F}_{q^m} = \mathbb{F}_q$:

Let $\alpha \in L^{(h)} \cap \mathbb{F}_{q^m}$. We have that $\alpha^q = \sigma(\alpha)$ because $\alpha \in \mathbb{F}_{q^m}$ and $\sigma|_{\mathbb{F}_{q^m}}$ is the Frobenius.

Since $\alpha \in L^{(h)}$ we get $\sigma \circ h(\alpha) = \alpha$. But $\sigma \circ h(\alpha) = \sigma(\alpha)$. So, from both equations, we get $\alpha^q = \alpha$, so $\alpha \in \mathbb{F}_q$.

$L^{(h)}$ is transcendental over $\mathbb{F}_q$:

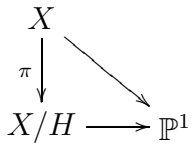
To prove this, let's prove that $\sigma \circ h$ has finite order.

$\sigma|_L = \mathrm{id}$, so σ and h commute on L. Also, $h|_{\mathbb{F}_{q^m}} = id$, so σ and h commute on $\mathbb{F}_{q^m}$. Hence σ and h commute on L'. Since σ and h have finite order, this implies that $\sigma \circ h$ has finite order.

$L^{(h)}\mathbb{F}_{q^m} = L'$: we leave as an exercise. □

So let's go back to the proof of the theorem. Now, $L^{(h)}\mathbb{F}_{q^m} = L' \Rightarrow X^{(h)}$ is isomorphic to X over $\mathbb{F}_{q^m}$.

$L = \{z : X \to \mathbb{P}^1\}$



For L' we have the same picture over $\mathbb{F}_{q^m}$.

Suppose we have a point $P_1 \in X(\overline{\mathbb{F}_q})$ and that $\pi(P_1) \in X/H(\mathbb{F}_q)$. This implies that $\pi(\sigma(P_1)) = \pi(P_1)$, which implies that $\sigma(P_1) = h(P_1)$ for some $h \in H$.

If the orbit of P_1 has m points then h is unique.

$z \in L'$, $\sigma(x_i(P_1)) = x_i(\sigma(P_1))$

$\sigma(z(P_1)) = \sigma(z)(\sigma(P_1)) = \sigma(z)(h(P_1)) = (h \circ \sigma)(z)(P_1)$

If $h \circ \sigma(z) = z$ (i.e $z \in L^{(h)}$) then $\sigma(z(P_1)) = z(P_1) \Rightarrow z(P_1) \in \mathbb{F}_q$.

Also, $P_1 \in X^{(h)}(\mathbb{F}_q) \Leftrightarrow \sigma(P_1) = h(P_1)$ (assuming that $P_1 \in X(\overline{\mathbb{F}_q})$ and $\pi(P_1) \in X/H(\mathbb{F}_q)$).

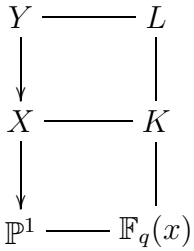
Exercise 11.1. Prove that $L' = L^{(h)}\mathbb{F}_{q^m}$. For this, it is enough to prove that $L' = L^{(h)}(K\mathbb{F}_{q^m})$, since $K \subset L^{(h)}$ (observe that $K\mathbb{F}_{q^m} = (L')^H$). Hint: Use Galois theory.

Example 11.6. Curves of the type $y^m = f(x)$ with $(m, p) = 1$, where p is the characteristic of the field, correspond to Kummer extensions, and curves of the type $y^p - y = f(x)$ with p the characteristic of the field correspond to Artin-Schreier extensions.

Twists of $y^m = f(x)$ are of the form $y^m = cf(x)$, where c is a generator of some coset of $({\mathbb{F}_q}^*)^m$ in ${\mathbb{F}_q}^*$. Twists of $y^p - y = f(x)$ are of the form $y^p - y = f(x) + c$, where c is a generator of a coset of $\wp(\alpha) = \alpha^p - \alpha$, $\wp(\mathbb{F}_q)$ in $\mathbb{F}_q$.

Back to the proof:

We have a curve $X/\mathbb{F}_q$, K the function field of X. Let L be the Galois closure of $K/\mathbb{F}_q(x)$. So L is the function field of some Y.



We proved that $\#Y^{(g)}(\mathbb{F}_q) \leq q + cq^{1/2}$. Also $\exists\ c > 0$, $d \geq 1$ such that, for all n,

$$\#Y^{(g)}(\mathbb{F}_{q^{nd}}) \leq q^{nd} + cq^{\frac{nd}{2}} \ .$$

Then

$$\frac{1}{|G|}\sum_{g\in G} \#Y^{(g)}(\mathbb{F}_{q^{nd}}) = \#\mathbb{P}^1(\mathbb{F}_{q^{nd}}) = q^{nd} + 1 \Rightarrow$$

$$\#Y^{(g)}(\mathbb{F}_{q^{nd}}) \geq q^{nd} - c'q^{\frac{nd}{2}} \ .$$

$$\frac{1}{|H|}\sum_{h\in H} \#Y^{(h)}(\mathbb{F}_{q^{nd}}) = \#X(\mathbb{F}_{q^{nd}}) \geq q^{nd} - c''q^{\frac{nd}{2}} \ ,$$

where $c' = c(|G| - 1)$ and $c'' = c\frac{(|G|-1)}{|H|}$.

□

Exercise 11.2. Let V be a vector space over a field $K, \mathrm{char}(K) = 0$, G a finite group acting on V, $\phi : V \to V$ such that ϕ commutes with G. Then

$$\frac{1}{|G|}\sum_{g\in G} \mathrm{Tr}(\phi \circ g) = \mathrm{Tr}(\phi|_{V^G}) \ ,$$

where $V^G = \{v \in V | gv = v, \forall g \in G\}$.

This exercise can be used to give a cohomological proof of the theorem.

12. Week Twelve

If X is a curve over $\mathbb{F}_q$ of genus g, then the Riemann hypothesis tells us that

$$\#X(\mathbb{F}_q) \leq q + 1 + 2\,g\,q^{1/2}.$$

But, in the proof we were not concerned with the constants, and so we can try to improve this bound.

Definition 12.1. Assume that q is odd. A *hyperelliptic curve* over $\mathbb{F}_q$, say X, is a curve given by an equation of the form $y^2 = f(x)$ where $f \in \mathbb{F}_q[x]$, with no repeated roots, i.e., the curve is smooth in the affine plane.

We actually consider the projective closure of these curves, but note that the point (or points) at infinity is (or are) singular.

Counting just affine points, we have:

$$\#\{y^2 = f(x) \mid x, y \in \mathbb{F}_q\} = \#\{f(x) = 0 \mid x \in \mathbb{F}_q\} + 2 \cdot \#\{f(x) \in (\mathbb{F}_q^\times)^2 \mid x \in \mathbb{F}_q\} \ .$$

On a non-singular model (i.e., a non-singular curve with the same function field), if d is odd, then the curve has one point at infinity. If d is even, it has two points at infinity. The points at infinity are $\mathbb{F}_q$ rational if and only if the leading coefficient of f is a square.

Using the Riemann-Roch theorem, one can prove that, if $\deg f = d$, the genus g of the curve is

$$g = \begin{cases} \dfrac{d-1}{2}, & \text{if } d \text{ is odd} \\ \dfrac{d-2}{2}, & \text{if } d \text{ is even .} \end{cases}$$

With the same notation from the previous lectures, let's choose $y_i = x^i$, for $i = 1, \ldots, n-1$ and $y_n = y$ (for some chosen n). Then

$$\begin{aligned} W &= \det \begin{pmatrix} y_1^q - y_1 & \cdots & y_n^q - y_n \\ Dy_1 & \cdots & Dy_n \\ \vdots & \ddots & \vdots \\ D^{(n-1)}y_1 & \cdots & D^{(n-1)}y_n \end{pmatrix} \\ &= y^q - y - \sum_{i=1}^{n-1} D^{(i)}y (x^q - x)^i \ . \end{aligned}$$

We know that W has a zero of order at least n at every rational point P of X with $x - x(P)$ being a local parameter (i.e., $f(x(P)) \neq 0$).

Lemma 12.2. *We have*

$$D^{(i)}y = \frac{F_i(x)}{y^{2i-1}}, \quad i \geq 1 \ ,$$

where $F_i(x) \in \mathbb{F}_q[x]$ and $\deg F_i(x) \leq i(d-1)$. Moreover, if a_i denotes the coefficient of $x^{i(d-1)}$ in $F_i(x)$, and α denotes the leading coefficient of $f(x)$, then, for $i < p$,

$$a_i = \frac{1}{i!} \prod_{j=0}^{i-1} \left(\frac{d}{2} - j\right) \alpha^i \ .$$

Proof. We prove the lemma by induction. For $i = 1$, applying D to both sides of $y^2 = f(x)$, we have $2\,y\,Dy = f'(x)$, i.e.,

$$Dy = \frac{f'(x)/2}{y} \ ,$$

and the formulas are true.

We prove the first part of the lemma first: suppose the lemma is true for $i - 1 \geq 1$. Then

$$D^{(i)}(y^2) = 2\,y\,D^{(i)}y + \sum_{j=1}^{i-1} D^{(j)}y\,D^{(i-j)}y = 2\,y\,D^{(i)}y + \sum_{j=1}^{i-1} \frac{F_j(x)F_{i-j}(x)}{y^{2i-2}} \ .$$

Note that $\deg(F_j(x)\,F_{i-j}(x)) \leq i(d-1)$ and $\deg(f(x)^{i-1}\,D^{(i)}f(x)) \leq i(d-1)$. So, defining

$$F_i(x) \equiv \frac{f(x)^{i-1}\,D^{(i)}f(x) - \sum_{j=1}^{i-1} F_j(x)F_{i-j}(x)}{2} \ ,$$

we have $\deg F_i(x) \le i(d-1)$ and

$$D^{(i)}y = \frac{F_i(x)}{y^{2i-1}} \ .$$

We now prove the part about the a_i's: assume the lemma true for $i-1 < p-1$. Then:

$$\begin{aligned} D^{(i)}y &= \frac{1}{i} D\big(D^{(i-1)}y\big) = \frac{1}{i}\, D\Big(\frac{F_{i-1}(x)}{y^{2i-3}}\Big) \\ &= \frac{1}{i}\left[\frac{DF_{i-1}(x)\, y^{2i-3} - F_{i-1}(x)\,(2i-3)\, y^{2i-4}\, f'(x)/2y}{y^{4i-6}}\right] \\ &= \frac{1}{i}\left[\frac{DF_{i-1}(x)\, f(x) - F_{i-1}(x)\,(2i-3)\, f'(x)/2}{y^{2i-1}}\right] . \end{aligned}$$

The coefficient of $x^{i(d-1)}$ is then

$$\begin{aligned} a_i &= \frac{(i-1)(d-1)\, a_{i-1}\, \alpha - a_{i-1}\,(2i-3)\, d\, \alpha/2}{i} \\ &= \frac{\alpha}{i}\Big(\frac{d}{2} - (i-1)\Big)\, a_{i-1} \ . \end{aligned}$$

Since $a_1 = \alpha\, d/2$, one deduces that a_i is as in the statement of the lemma.
(Note that we could use this argument to prove the first part of the lemma for $i < p$.)
□

Therefore, multiplying W by y^{2n-3} (to clear denominators), we have

$$\begin{aligned} P := y^{2n-3}\, W &= y^{2n-3}(y^q - y) - \sum_{i=1}^{n-1} F_i(x)\, y^{2n-2i-2}\, (x^q - x)^i \\ &= f(x)^{n+(q-3)/2} - f(x)^{n-1} - \sum_{i=1}^{n-1} F_i(x)\, f(x)^{n-i-1}\, (x^q - x)^i \ . \end{aligned}$$

Then, P is a polynomial in x with a zero of order greater than or equal to n for every $x \in \mathbb{F}_q$, such that $f(x) \in (\mathbb{F}_q^\times)^2$ (since W does and $y \neq 0$ for such x's) and a zero of order at least $n-1$ if $x \in \mathbb{F}_q$ with $f(x) = 0$.

Also, since

$$\begin{aligned} \deg F_i(x)\, f(x)^{n-i-1}\, (x^q - x)^i &\le i\,(d-1) + d\,(n-i-1) + q\, i \\ &= (q-1)\, i + d\,(n-1) \le (q-1)\,(n-1) + d\,(n-1) \ , \end{aligned}$$

we have,

$$\deg P \le \max\left\{ d\Big(n + \frac{q-3}{2}\Big), (n-1)(q+d-1) \right\}$$

If $P \not\equiv 0$, we get:

$$n\, \#\{x \in \mathbb{F}_q :\, f(x) \in (\mathbb{F}_q^\times)^2\} + (n-1)\, \#\{x \in \mathbb{F}_q :\, f(x) = 0\} \le \deg P \ .$$

Ignoring the $f(x) = 0$ part:

$$\#\{x \in \mathbb{F}_q : f(x) \in (\mathbb{F}_q^\times)^2\} \leq \frac{\max\{d\,(n + (q-3)/2), (n-1)(q+d-1)\}}{n} \ .$$

The best n is $\lfloor d/2 - 1 \rfloor$. We get a bound of the form $(q - 1 + d)\, d/(d+2)$, which implies that the number of points on the curve is less than or equal to $2(q-1+d)\, d/(d+2) + d$ (the two terms in the maximum above are approximately equal).

This beats the Weil bound if, roughly, $d > q^{1/2}$. It beats the trivial bound $(2d+2)$ if $d < \sqrt{2q}$.

Now, if $P \equiv 0$, then $W \equiv 0$, what implies:

$$y^q - y = \sum_{i=1}^{n-1} (D^{(i)} y)\, (x^q - x)^i \ .$$

So, if $x \in \mathbb{F}_q$, with $f(x) = 0$, we get $y \in \mathbb{F}_q$ (since the poles of $D^{(i)} y$ occur where $f(x) = 0$). Thus:

$$\#\{x \in \mathbb{F}_q : f(x) \in (\mathbb{F}_q^\times)^2\} \geq q - d \ .$$

Lemma 12.3. *If $W \equiv 0$, then $n\, D^{(n)} y \equiv 0$.*

Proof. We have

$$W = y^q - y - \sum_{i=1}^{n-1} D^{(i)} y\, (x^q - x)^i \equiv 0 \ ,$$

what implies:

$$\begin{aligned} 0 \equiv DW &= -Dy - \sum_{i=1}^{n-1} \left[(i+1) D^{(i+1)} y\, (x^q - x)^i + D^{(i)} y\, i\, (x^q - x)^{(i-1)}\, (-1) \right] \\ &= n\, D^{(n)} y\, (x^q - x)^n \ , \end{aligned}$$

since the sum is telescoping. Thus, $nD^{(n)} y \equiv 0$.

Moreover, we have that $D^{(n)} y \not\equiv 0$ if $n < d/2 < p$. Indeed, by lemma 12.2,

$$a_n = \frac{1}{n!} \prod_{i=0}^{n-1} \left(\frac{d}{2} - i \right) \alpha^n .$$

We always have $\alpha^n \neq 0$, and if $n < p$, then $n! \neq 0$. Also, since $n < d/2 < p$, $\prod_{i=0}^{n-1} (d/2 - i) \neq 0$. Hence, in this situation, $a_n \neq 0$ and so $D^{(n)} y \not\equiv 0$. Then, if $n < d/2 < p$, by lemma 12.3 we have that $W \not\equiv 0$. □

Theorem 12.4 (Lang-Weil)**.** *Let $X \subset \mathbb{P}^N$ be an absolutely irreducible variety defined over $\mathbb{F}_q$ of dimension n and degree d. Then, there exists $c_1, c_2 \in \mathbb{Z}$, depending on n and d, such that*

$$|\#X(\mathbb{F}_q) - q^n| \leq c_1\, q^{n-1/2} + c_2 \ .$$

We will prove the theorem for the case of $X \subset \mathbb{P}^3$, smooth of dimension 2, also trying to get good c_1 and c_2. Such X is given by zeros of a single homogeneous polynomial $f(x_0, x_1, x_2, x_3) \in \mathbb{F}_q[x_0, x_1, x_2, x_3]$ of degree d, and such that for any $P \in X$, there exists an $i \in \{0, 1, 2, 3\}$, such that $(\partial f/\partial x_i)(P) \neq 0$.

We denote the plane

$$\sum_{i=0}^{3} \frac{\partial f}{\partial x_i}(P)\, x_i = 0$$

by $T_P X$, and we call if the **tangent plane** to X at P.

In this case, Deligne tells us that

$$\#X(\mathbb{F}_q) = q^2 + 1 + \sum_{i=1}^{b_1} \big(\alpha_i + \frac{q^2}{\alpha_i}\big) + \sum_{i=1}^{b_2} \beta_i \ ,$$

where $|\alpha_i| = q^{1/2}$ and $|\beta_i| = q$. Thus,

$$|\#X(\mathbb{F}_q) - (q^2 + 1)| \leq b_1(q^{3/2} + q^{1/2}) + b_1\, q \ .$$

In $\mathbb{P}^3$, we have $b_1 = 0$ and $b_2 = (d^3 - 4d^2 + 6d - 2)$, and the bound reduces to

$$|\#X(\mathbb{F}_q) - (q^2 + 1)| \leq q\,(d^3 - 4d^2 + 6d - 2) \ .$$

Now, let's fix a line L and consider all planes $H \supset L$. For each such H we will look at $X \cap H$.

The case $d = 1$ is trivial.

So, we can assume $d \geq 2$ and then $X \neq H$ for any H, and so $X \cap H$ is a curve.

We can choose coordinates such that

$$L : \ x_2 = x_3 = 0.$$

Thus, $H \supset L$ has the form

$$H : \ x_3 = \lambda x_2, \quad \text{for some } \lambda \in \mathbb{F}_q$$

or

$$H : \ x_2 = 0 \ .$$

Therefore, planes containing a fixed line form a $\mathbb{P}^1$. Then, there are exactly $q + 1$ such planes defined over $\mathbb{F}_q$.

The intersection $X \cap H$ is given by the equation

$$\begin{cases} x_3 = \lambda\, x_2 \\ f(x_0, x_1, x_2, x_3) = 0 \end{cases} \qquad \text{or} \qquad \begin{cases} x_3 = \lambda\, x_2 \\ f(x_0, x_1, x_2, \lambda\, x_2) = 0 \end{cases}$$

or

$$\begin{cases} x_2 = 0 \\ f(x_0, x_1, x_2, x_3) = 0 \end{cases} \qquad \text{or} \qquad \begin{cases} x_2 = 0 \\ f(x_0, x_1, 0, x_3) = 0 \end{cases}$$

Note that $f(x_0, x_1, x_2, \lambda\, x_2) = 0$ (or $f(x_0, x_1, 0, x_3) = 0$) define a plane curve of degree d. We need to understand how often this curve is smooth.

Lemma 12.5. *The intersection $X \cap H$ is singular at P if and only if $H = T_P X$. (Remember that X is smooth, and then the tangent plane is well-defined. Also, this theorem is true for arbitrary fields.)*

Proof. Assume that $X \cap H$ is singular at a point P. We can choose coordinates so that $P = (0:0:0:1)$ and H is given by $x_0 = 0$. Then, the equation of $X \cap H$ is

$$f(0, x_1, x_2, x_3) = 0 \quad (\text{in } H).$$

Since P is singular, we have

$$\frac{\partial f}{\partial x_1}(0:0:0:1) = \frac{\partial f}{\partial x_2}(0:0:0:1) = \frac{\partial f}{\partial x_3}(0:0:0:1) = 0 \ .$$

Then, $T_P X$ is given by

$$\frac{\partial f}{\partial x_0}(0:0:0:1)\, x_0 = 0 \ ,$$

or $x_0 = 0$, since $\frac{\partial f}{\partial x_0}(0:0:0:1)$ is non-zero by hypothesis, and thus $T_P X = H$.

Conversely, assume that $H = T_P X$ for some P. Change the coordinates such that $P = (0:0:0:1)$ and $H = T_P X$ is given by $x_0 = 0$. This implies that

$$\frac{\partial f}{\partial x_1}(0:0:0:1) = \frac{\partial f}{\partial x_2}(0:0:0:1) = \frac{\partial f}{\partial x_3}(0:0:0:1) = 0 \ ,$$

which implies that $f(0, x_1, x_2, x_3) = 0$ (i.e., $X \cap H$) is singular at P.

□

Remember that the set of all planes in $\mathbb{P}^3$ is the dual $(\mathbb{P}^3)^* \cong \mathbb{P}^3$. We have then the map $\phi : X \to (\mathbb{P}^3)^*$ defined by

$$\phi(P) = T_P X = \left(\frac{\partial f}{\partial x_0}(P) : \frac{\partial f}{\partial x_1}(P) : \frac{\partial f}{\partial x_2}(P) : \frac{\partial f}{\partial x_3}(P) \right) .$$

Define $X^* \equiv \phi(X)$ and $d^* \equiv \deg X^*$. Since X^* is the image of X under ϕ, we have $\dim X^* \leq \dim X = 2$.

If $L \subset \mathbb{P}^3$ is a line, the set

$$\{H \supset L : H \text{ is a plane}\}$$

is a line, say $L^* \subset (\mathbb{P}^3)^*$. (As we have mentioned before, the planes through a line forms a line. For instance, if L is $x_0 = x_1 = 0$ in $\mathbb{P}^3$, then L^* is given by $x_2 = x_3 = 0$ in $(\mathbb{P}^3)^*$.)

We will now see that the non-smooth planes $H \supset L$ correspond to $L^* \cap X^*$. We need to pick an L such that $L \not\subset X$. We will prove this later.

So, if we pick L such that $L^* \not\subset X^*$ (we will also prove that we can pick such L later), then by Bezout's theorem $\# X^* \cap L^* \leq d^*$, and these are the non-smooth planes. Then,

$$\#X(\mathbb{F}_q) = \sum_{\substack{H \supset L \\ H \text{ over } \mathbb{F}_q}} \#(X \cap H)(\mathbb{F}_q) - q\,\#(X \cap L)(\mathbb{F}_q) =$$

$$\sum_{\substack{H \cap X \\ \text{smooth}}} \#(X \cap H)(\mathbb{F}_q) + \sum_{\substack{H \cap X \\ \text{non-sm.}}} \#(X \cap H)(\mathbb{F}_q) - q\,\#(X \cap L)(\mathbb{F}_q).$$

If $X \cap H$ is a smooth plane curve, then we sketched the proof that the genus of this curve is $(d-1)(d-2)/2$, and so, by the Riemann Hypothesis,

$$q+1-(d-1)(d-2)q^{1/2} \leq \#X \cap H(\mathbb{F}_q) \leq q+1+(d-1)(d-2)q^{1/2} \ .$$

If $X \cap H$ is not smooth, $X \cap H$ is still a plane curve of degree d, and we have the trivial bounds

$$0 \leq \#X \cap H(\mathbb{F}_q) \leq d(q+1).$$

Also, by Bezout's theorem,

$$0 \leq \#X \cap L(\mathbb{F}_q) \leq \#X \cap L \leq d$$

(since $L \not\subset X$).

Hence

$$\begin{aligned} \#X(\mathbb{F}_q) &\leq (q+1)(q+1+(d-1)(d-2)q^{1/2}) + d^* d(q+1) - 0 \\ &\leq q^2 + (2(d-1)(d-2) + (d\,d^* + 2) + d\,d^* + 1)q^{3/2} \end{aligned}$$

and

$$\#X(\mathbb{F}_q) \geq (q+1-d^*)(q+1-(d-1)(d-2)q^{1/2}) - dq \ .$$

13. Week Thirteen

We are proving the Lang-Weil estimate for smooth surfaces X in $\mathbb{P}^3$. We assume that X is defined over $\mathbb{F}_q$, and that X is given by the homogeneous polynomial $f \in \mathbb{F}_q[x_0, x_1, x_2, x_3]$. We also have a map

$$\phi : X \to (\mathbb{P}^3)^*$$

given by

$$P \mapsto T_P X = \Big(\frac{\partial f}{\partial x_0}(P) : \frac{\partial f}{\partial x_1}(P) : \frac{\partial f}{\partial x_2}(P) : \frac{\partial f}{\partial x_3}(P)\Big) \ ,$$

where $T_P X$ is the tangent plane to X at the point P. We let $X^* = \phi(X)$. The statement of the theorem is the following:

Theorem 13.1 (Lang-Weil)**.** *There exist constants $C_1(d), C_2(d)$ depending only on the degree d such that*

$$|\#X(\mathbb{F}_q) - q^2| \leq C_1(d)q^{3/2} + C_2(d) \ .$$

Earlier in the semester we proved that we can replace the right hand side with the bound $3dq^2 + 2dq + 1$. If the constant C_2 is on the order of d^6, then the Lang-Weil is worse than the bound we proved earlier; thus we only consider small degrees d.

To finish our proof, we needed to establish three things. We needed a bound on $d^* = deg(X^*)$, we needed the existence of a line L in $\mathbb{P}^3$ defined over $\mathbb{F}_q$ such that $L \not\subseteq X$, and we needed this line to also have the property that $L^* \not\subseteq X^*$.

Lemma 13.2. *If d is the degree of X as above, then $d^* \leq d(d-1)^2$.*

Proof. We work over an algebraically closed field for this result. If we drop the hypothesis that the line L to be chosen be defined over $\mathbb{F}_q$, then it is easy to find a line not contained in X — pick a point not on the surface and draw any line through it. The same can also be done in $(\mathbb{P}^3)^*$. Take a line L_1 (defined over $\overline{\mathbb{F}_q}$) such that $L_1 \not\subseteq X^*$. For a generic such line, we know that

$$d^* = \#X^* \cap L_1 \ .$$

Changing coordinates, we may assume that L_1 is given by $x_2 = x_3 = 0$. Now count the points $P \in X$ such that $T_P X \supset L_1^*$. It is easy to see that $T_P X \supset L_1^*$ is equivalent to the conditions that $f(P) = 0$ and $\frac{\partial f}{\partial x_2}(P) = 0 = \frac{\partial f}{\partial x_3}(P)$. By Bezout, these three conditions give that $d^* \leq d(d-1)^2$. □

To show that we can find a line meeting the other conditions, we proceed as follows. First, we will find a plane $H/\mathbb{F}_q$ with H^* not an element of X^*, i.e., such that H is not tangent to X. Then we will find a point $P \in H(\mathbb{F}_q)$ with $P \notin X \cap H$. Then any line L contained in H which contains P will suffice. Since $H \supset L$ and H is a plane, we know that $H^* \in L^*$; since $H^* \notin X^*$, we know that $L^* \not\subseteq X^*$.

To prove that such an H^* exists, it is enough to show that $\#X^*(\mathbb{F}_q) < \#(\mathbb{P}^3)^*$ since we only need a plane not tangent to X, i.e., a point in $(\mathbb{P}^3)^*$ not on X^*. Using our old bound for the number of points on a surface, we get that

$$\#X^*(\mathbb{F}_q) \leq 3d^*q^2 + 2d^*q + 1 \leq 6d^3q^2 \ .$$

We also know that

$$\#(\mathbb{P}^3)^* = q^3 + q^2 + q + 1 > q^3 \ .$$

Thus if $q > 6d^3$, we can find such an H^*.

To find the point P, we must show that $\#X \cap H(\mathbb{F}_q) < \#H(\mathbb{F}_q)$. We know that

$$\#X \cap H(\mathbb{F}_q) \leq d(q+1),$$

and also that

$$\#H(\mathbb{F}_q) = q^2 + q + 1 > q^2 \ .$$

Thus the desired point P exists if $q > d + 1$. This finishes the proof of Lang-Weil in the case of smooth surfaces in $\mathbb{P}^3$. Note, however, that this argument was quite wasteful and produced bad constants $C_1(d), C_2(d)$.

For this result, we looked at $\#X \cap H$ with $X \cap H$ smooth for most planes H, but we only need to worry about those intersections which are not absolutely irreducible. But sometimes being reducible can actually help get a better bound. Assume there is a line $L \subset X$. Then $X \cap H \supset L$ if $H \supset L$. But we know about L, and $X \cap H = L \cup C_H$ where C_H is a curve of degree $d-1$. This leads to the following result.

Theorem 13.3. *Let X be a smooth surface of degree 3 in $\mathbb{P}^3$. Then there exists a constant $c > 0$ such that*

$$|\#X(\mathbb{F}_q) - q^2| \leq cq \ .$$

Proof. We will use the fact that every cubic over an algebraically closed field contains 27 lines. Strictly speaking, we need the line to be defined over $\mathbb{F}_q$; by going to a finite extension and using properties of the zeta function, we can deduce the general case. Since $d = 3$, the curves C_H have degree 2, so they are conics in the plane H. They are either smooth or the union of 2 lines. The latter happens at most 13 times since in that case $L \subset X$ would be one of 27 lines and then the other pairs of lines would also lie on X. We know that smooth conics have $q+1$ rational points, so in this case $\#C_H(\mathbb{F}_q) = q+1$. We also know that

$$0 \leq \#C_H \cap L(\mathbb{F}_q) \leq 2 \ .$$

This gives

$$\#X(\mathbb{F}_q) = \#L(\mathbb{F}_q) + \sum_{H \supset L} \#(C_H \setminus L)(\mathbb{F}_q) \ ,$$

where we can split this last sum into the sum over planes H which intersect in a smooth conic and planes H that intersect in two lines. We know that $\#L(\mathbb{F}_q) = q+1$, and also that the total number of points on $C_H \setminus L$ for H intersecting X in two lines is on the order of q since this happens at most 13 times for between $2q$ and $2q+2$ points each time. If H intersects X in a smooth conic, then the sum

$$\sum_{H \text{ good}} \#(C_H \setminus L)(\mathbb{F}_q)$$

simplifies to the number of "good" planes times q plus something on the order of a constant. The number of "good" planes is between $q-12$ and $q+1$, so is itself of the form $q + O(1)$; this gives that the total sum is of the form $q^2 + O(q)$. □