Counting Points on Varieties and Applications to Ranks of Elliptic Curves over Function Fields

Worksheet for Week 1 and 2

Ben Church and Spencer Dembner

June 24, 2023

Problems marked with $*$ are very hard. Feel free to move on without fully solving them.

1 Rationality and Unirationality

We say that the variety X defined by a polynomial $f \in k[x_0, \dots, x_n]$ is *rational* if f can be "solved by rational functions". Explicitly this means there exist rational functions $r_0, \dots, r_n \in k(t_1, \dots, t_n)$ in n indeterminants such that,

$$f(r_1(t_1, \dots, t_n), \dots, r_n(t_1, \dots, t_n)) = 0$$

such that every indeterminants t_i appears in some r_j. We are now going to make this more precise by looking at the field of fractions of the ring where we set $f = 0$:

$$K = \mathrm{Frac}\left(k[x_0, \dots, x_n]/(f)\right)$$

Definition 1.0.1. We say that a finitely generated field K/k is,

(a) *rational* if $K \cong k(t_1, \dots, t_n)$ for some indeterminants $t_1, \dots, t_n$

(b) *unirational* if $K \subset k(t_1, \dots, t_n)$ for some indeterminants $t_1, \dots, t_n$

Example 1.0.2. The function field of the variety defined by,

$$x_0 + f(x_1, \dots, x_n) = 0$$

for any polynomial f not depending on x_0 is always rational. Indeed, we eliminate x_0,

$$x_0 = -f(x_1, \dots, x_n)$$

and thus,

$$K = k(x_1, \dots, x_n)$$

Example 1.0.3. The fraction field of,

$$y^2 = x^3$$

is rational. Indeed,

$$K = k(\tfrac{y}{x})$$

because $x = (\frac{y}{x})^2$ and $y = (\frac{y}{x})^3$.

In the following problems let k be an algebraically closed field (and of characteristic not $2, 3$).

1.1

Show that the function field of,

$$x^2 + y^2 = 1$$

is rational. What about the function field of,

$$x_0^2 + x_1^2 + \cdots + x_n^2 = 1$$

What about the function field of the equation,

$$q(x_0, \dots, x_n) = 1$$

for any quadratic form q with coefficents in k.

1.2

Show that the function field of the cubic equation,

$$x^3 + y^3 = 1$$

is *not* rational. Hint: we're trying to solve $x^3 + y^3 = z^3$ in $k[t]$. Write,

$$x^3 = z^3 - y^3 = (z - y)(z - \zeta_3 y)(z - \zeta_3^2 y)$$

Use the fact that $k[t]$ is a UFD so we can assume that y, z are coprime.

1.3

Show that the function field of the cubic equation,

$$y^2 = f(x) = x^3 + ax + b$$

is rational if and only if f has a repeated root. Hint: consider derivatives of the parametrizing functions and their roots.

2 Luroth and Shioda

The Luroth problem asks when it being rational and unirational are equivalent for a function field K over an algebraically closed field k. We call the transcendence degree $\text{trdeg}_k(K)$ the *dimension* of the field K.

Theorem 2.0.1 (Luroth, Castelnuovo, and others)**.** If k has characteristic zero and $\text{trdeg}_k(K) \le 2$ then the following are equivalent,

(a) K is rational

(b) K is unirational

2.1

Show that the function field defined by,

$$x^3 + y^3 + z^3 = 1$$

is unirational. Hint: choose two lines, for example parametrically,

$$(x, y, z) = (t, -t, 1) \quad (x, y, z) = (s, -s, \zeta_3)$$

For fixed t, s call the points on these lines P and Q respectively. Now the claim is that the line $\overline{PQ}$ intersects the cubic equation in exactly one point besides P and Q. Mapping (t, s) to this point will give the desired parametrization.

2.2 $*$

Show that the function field defined by,

$$x^3 + y^3 + z^3 + w^3 = 1$$

is *unirational.* Hint: choose a line satisfying the equation and consider the planes passing through this line. They are parametrized by two numbers s, t. The intersection of each plane with the cubic equation factors into a linear equation and a quadratic part. If you allow square roots in some polynomials in s, t you should be able to parametrize the residual quadratic part with an additional variable.

It is a very difficult theorem due to Clemens and Griffiths that the function field in this example is *NOT* rational.

2.3

In characteristic p very weird things can happen. Consider the Zariski surface X,

$$z^p = f(x, y)$$

where $f \in k[x, y]$ over a field k of characteristic p. Show that X is unirational. Hint: consider $x = t^p$ and $y = s^p$, how can you exploit that k has characteristic p.

Example 2.3.1. Consider the Fermat surface X defined by,

$$x^n + y^n + z^n = 1$$

over the field $k = \overline{\mathbb{F}}_p$. Shioda proves [**shioda_fermat**] that X is unirational if and only if,

$$p^\nu \equiv -1 \mod n$$

for some positive integer ν. This will be our main motivating example.

3 Counting Points over $\mathbb{F}_q$

Let $q = p^n$ be a power of a prime p.
Suppose we have a polynomial, $f \in \mathbb{F}_q[x_1, \ldots, x_n]$ with coefficients in the finite field $\mathbb{F}_q$. Let X be the *variety* defined by f. An interesting sequence of numbers associated to X are the counts of the number of solutions to f in each of the larger fields $\mathbb{F}_q$,

$$\#X(\mathbb{F}_{q^n}) = \#\{(x_1, \ldots, x_n) \in \mathbb{F}_{q^n} \mid f(x_1, \ldots, x_n) = 0\}$$

To analyze the behavior of this sequence, we put it into an exponential generating function called the *zeta function* of X,

$$\zeta_X(t) = \exp\left(\sum_{n \geq 1} \frac{\#X(\mathbb{F}_{q^n})}{n} t^n\right)$$

3.1

Let $X = \mathbb{A}^n_{\mathbb{F}_q}$ You can think of this as the case where $f = 0$ in the above definition. Then compute $\zeta_X(t)$. You should find that it simplifies and has a pole at $t = q^{-n}$.

3.2

Let $a_0, a_1, \ldots, a_r \in \mathbb{F}_q$. How many solutions are there to the equation,

$$a_0 x_0 + a_1 x_1 + \cdots + a_r x_r = 0$$

in the field $\mathbb{F}_q$ meaning the number $\#X(\mathbb{F}_q)$ for the above equation? Compute ζ_X.

3.3

Let $u \in \mathbb{F}_q$ and $n > 0$ be an integer, and let $d = \gcd(n, q-1)$. Show that the number $N(u)$ of solutions to the equation $x^n = u$ is,

$$N(u) = \begin{cases} 1 & u = 0 \\ d & u \neq 0 \text{ and admits a d-th root in } \mathbb{F}_q \\ 0 & u \neq 0 \text{ and does not admit a d-th root in } \mathbb{F}_q \end{cases}$$

Notice that unlike the previous cases, the number of points $\#X(\mathbb{F}_q) = N(u)$ for $X = V(x^n - u)$ is not a polynomial in q. Compute ζ_X.

3.4

You may take on faith the following fact: consider a polynomial,

$$y^2 - f(x) \in \mathbb{F}_p[x, y]$$

with f monic[1] of degree d. Set,

$$\delta = \begin{cases} 1 & d \text{ is odd} \\ 2 & d \text{ is even} \end{cases} \qquad g = \begin{cases} \frac{d-1}{2} & d \text{ is odd} \\ \frac{d}{2} & d \text{ is even} \end{cases}$$

[1] This assumption ensures that the "points at ∞" are defined over $\mathbb{F}_p$.

Set $X = V(f)$. This is called the "an affine hyperelliptic curve of genus g". Then,

$$\zeta_X(t) = \frac{P(t)}{(1-t)^{1-\delta}(1-pt)}$$

where $P(t)$ is a monic polynomial of degree $2g$ with constant term p^g.

(a) What does this form of ζ_X imply explicitly about the point counts $\#X(\mathbb{F}_{p^n})$?

(b) consider $f(x) = x^3 + 1$ compute ζ_X for $p = 5, 7$

(c) consider $f(x) = x^4 - x^2 + x$ compute ζ_X for $p = 5, 7$

(d) Write a program in sage that takes in a polynomial $f \in k[x]$ and a prime number p and computes ζ_X for $y^2 - f$ over $\mathbb{F}_p$.

4 The Weil Conjectures

You probably noticed that all the zeta functions we computed are all rational functions. This is not a coincidence. One of the crowning achievements of modern algebraic geometry is understanding the properties of this generating function in terms of the geometry of X. What I mean by the geometry of X is considering a lift the defining polynomial $f \in \mathbb{Z}[x_0, \ldots, x_n]$ to one with integer coefficients and considering the complex vanishing locus,

$$Z(f) = \{(x_1, \ldots, x_n) \in \mathbb{C}^n \mid f(x_0, \ldots, x_n) = 0 \subset \mathbb{C}^n$$

This is an actual geometric space. The main result says that ζ_X is a rational function of the form,

$$\zeta_X(t) = \frac{P_1(t) \cdots P_{2n-1}(t)}{P_p(t) \cdots P_{2n}(t)}$$

where $P_i(t)$ is a polynomial of degree b_i where,

$$b_i = \dim_{\mathbb{Q}} H_i(Z(f), \mathbb{Q})$$

is the dimension of the i^{th}-homology group of the complex variety $Z(f)$.
The Weil conjectures (now theorems) make precise predictions about the form of the ζ function. The best results are true for X a *non-singular projective* variety over $\mathbb{F}_q$. Non-singular means that the defining equations have full-rank partial derivatives everywhere. Projective means that the variety is "complete" e.g. that the associated variety over the complex numbers is a compact manifold. Then the Weil conjectures state that if X is an n-dimensional non-singular projective variety over $\mathbb{F}_q$ then,

(a) Rationality: $\zeta_X(t)$ is a *rational function* of t and takes the form,

$$\zeta_X(t) = \frac{P_1(t) \cdots P_{2n-1}(t)}{P_p(t) \cdots P_{2n}(t)}$$

where $P_i(t)$ is an integer polynomial. Furthermore, $P_0(t) = 1 - t$ and $P_{2n}(t) = 1 - q^n t$ and all $P_i(t)$ factor over $\mathbb{C}$ as,

$$\prod_j (1 - \alpha_{ij} t)$$

for numbers $\alpha_{in} \in \mathbb{C}$ called the *roots* of X

(b) Functional equation and Poincaré duality: The zeta function satisfies,

$$\zeta(X, q^{-n}t^{-1}) = \pm q^{ne/2}t^e\zeta(X, t)$$

where $e := e(X)$ is the *Euler characteristic* of X. In particular, for each i, the numbers $\{\alpha_{2n-i,j}\}_j$ and $\{q^n/\alpha_{i,j}\}_j$ are equal up to permutation.

(c) Riemann hypothesis: $|\alpha_{i,j}| = q^{i/2}$ for all $0 \leq i \leq 2n$ and all j.

(d) Betti numbers: if X is a "good reduction mod p" of a non-singular projective variety X_K over a number field $K \hookrightarrow \mathbb{C}$ embedded in $\mathbb{C}$ then,

$$\deg P_i = \dim_{\mathbb{C}} H_i(X_K(\mathbb{C}), \mathbb{Z})$$

which is the dimension of the homology of the complex manifold defined by the same equations as X.

The reason for the terminology "Riemann hypothesis" is the formal similarity to the Riemann hypothesis for the Riemann zeta function. Indeed, suppose we write,

$$\zeta_X(s) = \zeta_X(q^{-s})$$

Then the functional equation becomes,

$$\zeta_X(n - s) = \pm q^{ne/2-es}\zeta_X(s)$$

which looks similar to the functional equation for the Riemann zeta function and the "Riemann hypothesis" part of the Weil conjectures becomes that all the poles and zeros of $\zeta_X(s)$ lie on the "critical lines" of complex numbers s with real part $k/2$ for $k \in 0, 1, \ldots, 2n$.

You can learn more about the Weil conjectures in the following places (arranged somewhat in increasing order of complexity)

(a) `https://en.wikipedia.org/wiki/Weil_conjectures`

(b) `http://www.math.toronto.edu/~jacobt/Lecture1.pdf`

(c) `https://pagine.dm.unipi.it/tamas/Weil.pdf` Chapters 1 and 2

(d) `https://pages.uoregon.edu/ddugger/weil607.pdf` Chapters 1-4

(e) `https://people.math.harvard.edu/~mpopa/571/chapter2.pdf`

(f) `https://dept.math.lsa.umich.edu/~mmustata/zeta_book.pdf`.

In the following problems we will explore some examples of zeta functions of non-singular projective varieties.

4.1

We can write projective space as the quotient,

$$\mathbb{P}^n = \frac{\mathbb{A}^{n+1} \backslash \{0\}}{\mathbb{G}_m}$$

explicitly this means that the points over a field K are,

$$\mathbb{P}^n(K) = \frac{K^{n+1} \backslash \{0\}}{K^\times}$$

We can extend the definition of the ζ-function to these more interesting spaces by counting the number of points over the fields $\mathbb{F}_q$ using the above formula. Compute $\zeta_{\mathbb{P}^n}$ and compare to $\zeta_{\mathbb{A}^n}$.

4.2

Suppose that X decomposes as a disjoint union,

$$X = X_1 \sqcup X_2 \sqcup \cdots \sqcup X_k$$

of pieces. Prove that,

$$\zeta_X = \zeta_{X_1} \cdot \zeta_{X_2} \cdots \zeta_{X_k}$$

Use this to interpret geometrically the form of $\zeta_{\mathbb{P}^n}$.

4.3 *

Let $a, b, c \in \mathbb{F}_q$. How many non-zero solutions are there to the equation,

$$ax^2 + by^2 + cz^2 = 0$$

in $\mathbb{F}_{q^r}$ up to scaling? Call this number $S(r)$. Compute,

$$\zeta_X(t) = \exp\left(\sum_{r \geq 1} \frac{S(r)}{r} t^r\right)$$

and prove that it is a rational function. This is the zeta function of the variety $X = \frac{V(f) \backslash \{0\}}{\mathbb{G}_m}$.
Note that there are several cases, depending on whether or not $ax^2 + by^2 + cz^2$ is a product of linear factors over $\overline{\mathbb{F}_q}$. Does the zeta function satisfy the functional equation in each of these cases? Why or why not Can you compute the analogous zeta function for quadrics in more than three variables? Is the point count always a polynomial?
Hint: for the three-variable case, pick a point on the quadric – first you must show it has one – and look at a plane through this point. What does the intersection with the quadric look like? How many points does it have, up to scaling?

4.4

How many distinct k-dimensional subspaces of $\mathbb{F}_q^n$ are there? Call this number $R(q,k,n)$. Show that the function,

$$\zeta_{\mathrm{Gr}(k,n)}(t) := \exp\left(\sum_{r\geq 1} \frac{R(q^r,k,n)}{r} t^r\right)$$

is a rational function by computing it. This is the ζ function of the *Grassmannian* $\mathrm{Gr}(k,n)$ over $\mathbb{F}_q$. Check that this zeta function satisfies the functional equation part of the Weil conjectures i.e. that,

$$\zeta_{k,n}(q^{-d}t^{-1}) = \pm q^{de/2} t^e \zeta_{k,n}(t)$$

for appropriate integers d and e.

4.5

Consider the set $P_{n,d}$ of homogeneous degree d polynomials with coeffients in $\mathbb{F}_q$, in n variables. What is the *average* number of non-zero solutions to a polynomial in $P_{n,d}$, up to scaling?

4.6

Let $\{f_i\}$ be a system of polynomial equations with coefficients in $\mathbb{F}_q$, and let $X(\mathbb{F}_{q^k})$ be the set of solutions to $\{f_i\}$ in $\mathbb{F}_{q^k}$. The zeta function of the variety associated to this system of equations is,

$$\zeta_X(t) = \exp\left(\sum_{k\geq 1} \frac{\#X(\mathbb{F}_{q^k})}{k} t^k\right)$$

Write $\zeta_X(t)$ as an infinite product over the Galois orbits in,

$$X(\overline{\mathbb{F}}_q) = \bigcup_k X(\mathbb{F}_{q^k})$$

Write $\zeta_X(t)$ as an infinite sum over Galois orbits in $X(\overline{\mathbb{F}}_q)$.

4.7

Let X be a variety over $\mathbb{F}_q$. Then for any k we can "base change" it to a variety X' over $\mathbb{F}_{q^k}$. If X is defined by an equation $f \in \mathbb{F}_q[x_0,\ldots,x_n]$ then X' is simply defined by the same polynomial f but viewed as an element of $\mathbb{F}_q[x_0,\ldots,x_n]$. Explicitly, X' is characterized by the property that,

$$\#X'(\mathbb{F}_{(q^k)^n}) = \#X(\mathbb{F}_{q^{kn}})$$

What is the relationship between ζ_X and $\zeta_{X'}$? How can we compute the roots of X' in terms of the roots of X?

5 Supersingularity

We say that X is *supersingular* if all the roots of X are of the form $\zeta q^{\frac{i}{2}}$ where ζ is a root of unity. Part of the point of the project will be to find new examples of supersingular varieties.

One reason to care about supersingular varieties is the following conjecture. Shioda [**shioda_conjecture**] conjectured that, in the two dimensional case, X is rational if and only if X is supersingular. An overarching goal of this project is to test this conjecture. We do know the easy direction of this conjecture:

Proposition 5.0.1. If a variety X over $\mathbb{F}_q$ is unirational then X is supersingular.

This gives us already some examples of supersingular varieties. In the following problems we will find more examples.

5.1

Identify which of the varities considered previously are supersingular. Pay close attention to Problem 3.4. Does the supersingularity of a variety defined by a fixed polynomial $f \in \mathbb{Z}[x_0, \ldots, x_n]$ with integer coefficients considered over $\mathbb{F}_p$ for different primes p depend on the choice of prime?

5.2

Prove that a variety X over $\mathbb{F}_q$ is supersingular if and only if its base change (c.f. Problem 4.7) X' to $\mathbb{F}_{q^k}$ is supersingular.

6 Diagonal Hypersurfaces, Weil's Method, and Gauss Sums

Weil used a clever point counting method to check his conjectures for equations of the form,

$$a_0 x_0^{n_0} + a_1 x_1^{n_1} + \cdots + a_r a_r^{n_r} = 0$$

in the original paper where he first set out his clebrated conjectures:

`https://www.ams.org/journals/bull/1949-55-05/S0002-9904-1949-09219-4/S0002-9904-1949-09219-4.pdf`

This paper should be read in detail *after* you think about the following problems which develop Weil's point counting technique from scratch.

6.1

Let,

$$f(x_0, \ldots, x_n) = \sum_{i=0}^{n} a_i x^{m_i}$$

be a polynomial with coefficients $a_i \in \mathbb{F}_q$. Suppose that for each i, a_i is non-zero and has an m_i-th root in $\mathbb{F}_q$. Show that the zeta function of the variety $X = \{f = 0\}$ is independent of the a_i. In particular it is the same as the zeta function for the polynomial,

$$g(x_0, \ldots, x_n) = \sum_{i=0}^{n} x_i^{m_i}$$

6.2

The next problesm have to do with characters. A multiplicative character of $\mathbb{F}_q$ is a group homomorphism $\chi : \mathbb{F}_q^\times \to \mathbb{C}^\times$ from the nonzero elements of $\mathbb{F}_q$ to the nonzero elements of the complex numbers (both considered as groups under multiplication). Let $w \in \mathbb{F}_q^\times$ be a generator of the multiplicative group. Then any multiplicative character is determined by its value on w, which must be a $(q-1)$-th root of unity. Vice versa, for any rational number $\alpha \in \mathbb{Q}$ such that $(q-1)\alpha \in \mathbb{Z}$, we can define a character χ_α by setting,

$$\chi_\alpha(w) = e^{2\pi i\alpha}$$

We use the following convention: we regard any multiplicative character χ as a function $\chi : \mathbb{F}_q \to \mathbb{C}^\times$ by setting,

$$\chi(0) = \begin{cases} 0 & \chi \neq \chi_0 \\ 1 & \chi = \chi_0 \end{cases}$$

6.3

Show that if χ is a multiplicative character, then

$$\sum_{u \in \mathbb{F}_q} \chi(u) = \begin{cases} 0 & \chi \neq \chi_0 \\ q & \chi = \chi_0 \end{cases}$$

6.4

Show that the number $N(u)$ of solutions to $x^n = u$ defined in Problem 3.3 can be expressed as,

$$N(u) = \sum_{\substack{\alpha \in [0,1) \cap \mathbb{Q} \\ d\alpha \in \mathbb{Z}}} \chi_\alpha(u)$$

6.5

Let $a_0, a_1, \ldots, a_r \in \mathbb{F}_q$ and let $n_0, n_1, \ldots, n_r$ be positive integers. Let N_q be the number of solution to the equation,

$$a_0 x_0^{n_0} + a_1 x_1^{n_1} + \cdots + a_r a_r^{n_r} = 0$$

over $\mathbb{F}_q$. Set,

$$L(u) = \sum_{i=0}^{r} a_i u_i$$

and $d_i = \gcd(n_i, q-1)$. Then show that,

$$N_q = \sum_{u,\alpha} \chi_{\alpha_0}(u_i)\chi_{\alpha_1}(u_1) \cdots \chi_{\alpha_r}(u_r)$$

where the sum ranges over all $u = (u_0, \ldots, u_r)$ such that $L(u) = 0$ and all $\alpha = (\alpha_0, \ldots, \alpha_r)$ such that $\alpha_i \in [0,1)$ and $d_i\alpha_i \in \mathbb{Z}$ for all i.

6.6

We now break up the sum into two parts: the first where some $\alpha_i = 0$, the second where all $\alpha_i \neq 0$. For the given r-tuple of exponents n we define the set of admissible α,

$$A_{n,q} = \left\{(\alpha_0, \ldots, \alpha_r) : 0 < \alpha_i < 1 \text{ and } d_i \alpha_i \in \mathbb{Z} \text{ and } \sum \alpha_i \in \mathbb{Z} \text{ where } d_i = \gcd(n_i, q-1)\right\}$$

Assume all $a_i \neq 0$.

(a) Show using a change of variables $u_i \mapsto u_i / a_i$ that,

$$N_q = q^r + \sum_{\alpha \in A_{n,q}} \chi_{\alpha_0}(a_0^{-1}) \cdots \chi_{\alpha_r}(a_r^{-1}) S(\alpha)$$

where,

$$S(\alpha) = \sum_{\{u \mid \sum u_i = 0\}} \chi_{\alpha_0}(u_0) \cdots \chi_{\alpha_r}(u_r)$$

(b) Show that $S(\alpha)$ is divisible by $q - 1$. Then we define the Jacobi sum of α over $k = \mathbb{F}_q$ to be,

$$j(\alpha) = \frac{1}{q-1} S(\alpha)$$

7 Gaussian Sums

Let $k = \mathbb{F}_q$. Fix an additive character $\psi : k \to \mathbb{C}^\times$ and let $\chi : k^\times \to \mathbb{C}^\times$ be a nontrivial multiplicative character. Then we define the *Gaussian sum*,

$$g(\chi) := \sum_{x \in k} \chi(x) \psi(x)$$

Remember that when χ is nontrivial we set $\chi(0) = 0$ and otherwise $\chi_0(0) = 1$.

7.1

Show that $g(\chi_0) = 0$ and for $\chi \neq \chi_0$ we have,

$$g(\chi) \bar{g}(\chi) = q$$

7.2

Prove that $g(\chi)$ is independent of the choice of nontrivial additive character ψ up to multiplication by a root of unity. Hint: first prove the following lemma.

Lemma 7.2.1. Let R be a finite ring. If $\psi : R \to \mathbb{C}^\times$ is an additive character and $r \in R$ then set $\psi_r(x) = \psi(rx)$. Then the following are equivalent,

(a) ψ_r is nontrivial for all $r \neq 0$

(b) every additive character of R is of the form ψ_r for some $r \in R$.

Proof. Hint: let $\widehat{R}$ be the ring of additive characters (with pointwise addition and multiplication). Show that $R \to \widehat{R}$ via $r \mapsto \psi_r$ is a map of additive groups. What does it mean for this map to be injective or surjective? How does $\#R$ compare to $\#\widehat{R}$. $\square$

7.3

Prove that,

$$\chi(x) = \frac{g(\chi)}{q} \sum_{t \in k} \bar{\chi}(t) \bar{\psi}(tx)$$

which we think of as a Fourier expansion. Hint: use the fact that we can reindex the sum $g(\chi)$ to sum over tx for any fixed nonzero t.

7.4

Using the previous problem, prove that,

$$j(\alpha) = \frac{1}{q} g(\chi_{\alpha_0}) \cdots g(\chi_{\alpha_r})$$

Using this and previous problems, compute,

$$j(\alpha)\bar{j}(\alpha)$$