CTNT Summer School

Mini-course: Curves over finite fields

These notes contain the material from the lectures on Curves over Finite Fields. References and supplements for these notes are given at the end. There are some exercises in the body of the notes. Additional exercises will be added soon. Exercises that require some algebraic geometry background are marked with an (AG). There are optional 'exploratory' remarks, which direct the reader to topics of research in this area. These are marked with a ♟. If you find any errors, please let me know.

1 Lecture one: Elliptic curves over finite fields

Let $\mathbb{F}_q$ be the finite field with q elements, where q is a power of a prime $p > 0$. Recall that $\bar{\mathbb{F}}_q$ comes equipped with a map called the *Frobenius* map:

$$\sigma : a \mapsto a^q$$

and if $a \in \mathbb{F}_q$, then $a^q = a$.

Definition 1.1. We will define an elliptic curve E over $\mathbb{F}_q$ to be a curve defined by smooth plane cubic (a homogeneous polynomial of degree 3 in 3 variables) of the form:

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3, \tag{1}$$

where $a_i \in \mathbb{F}_q$ for all i.

Notation 1.2. If K is an extension of $\mathbb{F}_q$, we will let $E(K)$ denote the set of solutions to this equation in this extension.

One can also define an elliptic curve to be a smooth genus 1 curve, with an $\mathbb{F}_q$ rational point (we will define genus later). Any homogeneous polynomial $f(X_0, X_1 \dots X_n)$ of degree d can be *de-homogenized*, for instance by dividing by X_n^d and letting $x_i = X_i/X_n$.

Example 1.3. Let $f(X, Y, Z) = X^3 + Y^2Z + 2Z^3$. The dehomogenized version is $g(x, y) = x^3 + y^2 + 2$.

This process amounts to setting one of the variables to be 1. If you set $Z = 1$, equation 1 reduces to:

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{2}$$

If on the other hand, you set $Z = 0$, you get the point $[0 : 1 : 0]$ which we will call the point at ∞. Note that you don't really "see" the point at infinity on the dehomogenized equation.

Exercise 1. If $p \neq 2$, show that E can be given by $y^2 = f(x)$, where f has degree 3. If $p \neq 2, 3$ show that E is given by $y^2 = x^3 + Ax + B$ for some $A, B \in \mathbb{F}_q$. This is called the *short Weierstrass form*. If $p = 2$, show that E is given by $y^2 - y = h(x)$ for some rational function $h(x)$.

Exercise 2. (AG) If E is a genus 1 curve with a rational point, use Riemann Roch to show that E can be given by a plane cubic equation as in 2. Conversely, prove that a smooth plane cubic as in 1 has genus 1.

From now on, we will use the short Weierstrass form $E : y^2 = x^3 + Ax + B$, unless mentioned otherwise. The j invariant of this elliptic curve is defined as $j(E) := 1728\frac{4A^3}{4A^3+27B^2}$.

Exercise 3. Show that the smoothness of E amounts to saying $4A^3 + 27B^2 \neq 0$.

Since E is an algebraic variety (cut out by polynomial equations), one can consider the ring of functions on E, which we will denote by $k[E]$. Since E is given by $y^2 = x^3 + Ax + B$ on the affine patch $Z = 1$, it will do us no harm to think of $k[E]$ as $\mathbb{F}_q[x, y]/(y^2 - x^3 - Ax - B)$. We will denote by $k(E)$, the field of fractions of $k[E]$. This is called the *function field* of E.

Exercise 4. If you haven't seen much algebraic geometry before, this might be a useful exercise. Let $f : X \to Y$ be a map of two algebraic varieties over a field k. To start with, you can take these to be affine. That is, you can take the ring of functions on X, $k[X]$ to be the ring $k[x_0, x_1 \dots x_n]/I_1$ and $k[Y]$ to be $k[y_0, y_1 \dots y_m]/I_2$, where I_1 and I_2 are some ideals. Show that f induces a map of k-algebras $f^* : k[Y] \to k[X]$, and thus a map $f^* : k(Y) \to k(X)$. Further, if $X \to Y$ is dominant on $\bar{k}$ points (the closure of the image is all of Y), then the map $f^* : k(Y) \to k(X)$ is a field homomorphism. Thus in such cases, $k(Y)$ can be thought of as a subfield of $k(X)$.

Remark 1.4. If X and Y from the above exercise are curves, then any non-constant map induces an extension of function fields $k(Y) \hookrightarrow k(X)$. From now on, whenever we talk about maps of curves, we will generally be referring to non-constant maps, unless mentioned otherwise.

1.1 The Frobenius Twist

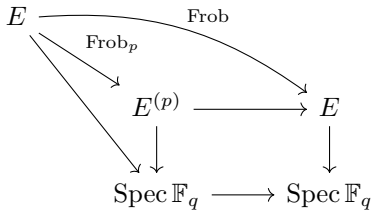
Define $E^{(p)}$ to be the elliptic curve given by the equation $y^2 = x^3 + A^p x + B^p$. Note that if $A, B \in \mathbb{F}_p$, then $E^{(p)} = E$. In general, we can give a map, which we will call Frob_p:

$$E \to E^{(p)}$$
$$(x, y) \mapsto (x^p, y^p).$$

Note that you can replace p here by any power of p to give a map $E \to E^{(p^r)}$. In particular, Frob_q acts on the elliptic curve $E/\mathbb{F}_q$ via $(x, y) \mapsto (x^q, y^q)$. Indeed if $y^2 = x^3 + Ax + B$, then $(y^q)^2 = (x^3 + Ax + B)^q = (x^q)^3 + A(x^q) + B$, since $A, B \in \mathbb{F}_q$.

Exercise 5. (AG) The absolute Frobenius morphism $\text{Frob} : E \mapsto E$ is the identity on points and the p-th power map on structure sheaves.

1. Show that this is a morphism of schemes.
2. Show that there is a commutative diagram as given below, i.e. the absolute Frobenius factors through the relative Frobenius Frob_p.



1.2 Number of points on an elliptic curve

Let $E/\mathbb{F}_q$ be given by $y^2 = x^3 + Ax + B$. We want to count the number of points: $E(\mathbb{F}_q)$. For a given $x \in \mathbb{F}_q$, whether or not $(x, y) \in E(\mathbb{F}_q)$ depends on the Legendre symbol:

$$a(x) := \left(\frac{x^3 + Ax + B}{q}\right).$$

Here the Legendre symbol is given by:

$$\left(\frac{b}{q}\right) = \begin{cases} 0 & \text{if } q|b \\ 1 & \text{if } b \text{ is a square} \mod q \\ -1 & \text{if } b \text{ is not a square} \mod q. \end{cases}$$

So the number of points is:

$$\sum_{x \in \mathbb{F}_q} (1 + a(x)) + 1.$$

The last 1 comes from the point at infinity. We will denote by a_q the sum $-\sum_{x \in \mathbb{F}_q} a(x)$. Then we have that:

$$\#E(\mathbb{F}_q) = q + 1 - a_q.$$

Theorem 1.5 (Hasse-Weil)**.** *The a_q's satisfy the following bound:*

$$|a_q| \leq 2\sqrt{q}.$$

Remark 1.6 (🚀)**.** Let E be an elliptic curve over $\mathbb{Q}$. At all but finitely many primes p, one E reduces to an elliptic curve E_p modulo p. The integers $a_p(E_p)$ arise as coefficients of a *modular form* $f = \sum_{n \geq 1} a_n q^n$. This is a consequence of the Shimura-Taniyama conjecture, now a theorem due to Wiles, colloquially called modularity. To read more about this, see: `https://www.ams.org/notices/199911/comm-darmon.pdf`.

1.3 The ℓ-torsion of an elliptic curve

Throughout this section, ℓ will be a prime not equal to p.

Fact 1.7. An elliptic curve comes equipped with a group structure.

Remark 1.8 (🚀)**.** If E is an elliptic curve over $\mathbb{Q}$, then the $\mathbb{R}$ points of E as well as the group law, have a very nice picture. It's a good way to get an idea of what the equations defining the group law should be in general. Over $\mathbb{C}$, an elliptic curve is a torus, i.e. there is a two dimensional $\mathbb{Z}$ lattice $\Lambda \subset \mathbb{C}$ such that $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$. This can be found in any standard book on elliptic curves (e.g. Silverman's book).

Definition 1.9. Let E and E' be two elliptic curves over $\mathbb{F}_q$. An isogeny $\phi : E \to E'$ is a group homomorphism that is surjective on $\bar{\mathbb{F}}_q$ points, and has finite geometric kernel. That is, $(\operatorname{Ker} \phi)(\bar{\mathbb{F}}_q)$ is finite.

Exercise 6. Consider the map $\phi : E \to E'$, and the induced map of function fields $\phi^* : k(E') \to k(E)$. We will define the degree of ϕ to be the degree of the field extension $[k(E') : k(E)]$. Show that if $\deg(\phi)$ is coprime to p, then it is equal to $|\operatorname{Ker}(\phi)(\bar{\mathbb{F}}_q)|$.

Example 1.10.

1. The map $[n] : E \to E$ sending P to $n \cdot P$ is an isogeny. If $n = 2$, then the non-trivial points in $\operatorname{Ker}([2])$ are given by the roots of $x^3 + Ax + B$. In general, the multiplication by $[n]$ map on E has degree n^2 and is defined by polynomial equations over $\mathbb{F}_q$.
2. The map $\operatorname{Frob}_p : E \to E^{(p)}$ is an isogeny of degree p.

The ($\bar{\mathbb{F}}_q$ points of the) n-torsion of E is defined as:

$$E[n] := \{P \in E(\bar{\mathbb{F}}_q) \mid [n] \cdot P = 0\}.$$

If $(n, p) = 1$, then $E[n] \cong (\mathbb{Z}/n\mathbb{Z})^2$.

1.3.1 The Tate module

Note that there are maps: $E[\ell^{n+1}] \to E[\ell^n]$ given by multiplication by ℓ. This allows us to form the inverse limit:

$$T_\ell(E) := \varprojlim_n E[\ell^n],$$

called the $\ell-$adic Tate module. Note that since $E[\ell^n] \cong (\mathbb{Z}/\ell^n\mathbb{Z})^2$, we have that $T_\ell(E) \cong \mathbb{Z}_\ell^2$.

One great advantage that the Tate module gives us is that it converts a lot of questions about the elliptic curve into questions about linear algebra. The action of Frob_q on E induces an action on $E[n]$ for each n, and therefore on the Tate module. We understand endomorphisms of $\mathbb{Z}_\ell^2$ much better. Let $\operatorname{Frob}_{q,\ell}$ denote the Frobenius acting of $T_\ell(E)$. Then this is given by a 2×2 matrix.

Fact 1.11. The characteristic polynomial of $\text{Frob}_{q,\ell}$ is given by:

$$P_{E,q}(T) := T^2 - a_q T + q.$$

One quick way of seeing why this might be true is notice that $\mathbb{F}_q$ points satisfy $(x^q, y^q) = (x, y)$. In particular, this means that Frob_q acts as the identity on $\mathbb{F}_q$ points. Setting $T = 1$ in the above equation gives you $E(\mathbb{F}_q)$.

Note that this is:

1. independent of ℓ.
2. integral, in particular showing that the eigenvalues of Frobenius are algebraic integers.

2 Curves of higher genus

A *curve* over $\mathbb{F}_q$ is an algebraic variety of (relative) dimension one. For now, we will only talk about smooth, geometrically integral and irreducible curves that can be embedded into projective space.

If you have a dominant map of two curves $\phi : C \to C'$, then the degree of ϕ is defined as the degree of the corresponding field extensions. As before, if the degree of the map is coprime to the characteristic of the field, then this is the same as the number of points in the preimage of any point (counted with multiplicity).

Example 2.1.

1. A *plane* curve of degree d is one that is defined by a homogeneous equation $f(X, Y, Z) = 0$ of degree d in $\mathbb{P}^2$. With such curves, we often set $Z = 1$ and work with the de-homogenized version $g(x, y) = \sum a_{ij} x^i y^j$. The intersections of $f(X, Y, Z) = 0$ with line $Z = 0$ are called the 'points at ∞.
2. A *hyperelliptic curve* C is a curve that has a degree 2 map to $\mathbb{P}^1$ given by $(x, y) \mapsto [x : 1]$. Away from characteristic 2, such a curve can be given by the equation:

   $$y^2 = f(x)$$

   for some squarefree polynomial $f(x)$. (Note: If the degree of f is higher than 4 than this equation is not smooth at ∞. However, it is *birational* to a smooth curve. In particular, the model $y^2 = f(x)$ captures enough of the arithmetic of the smooth curve. We choose this model because it's easier to work with).
3. An Artin-Schreier curve is a degree p cover of $\mathbb{P}^1$ in characteristic p. These are given by:

   $$y^p - y = f(x)$$

   where $f(x)$ is a rational function.

2.1 Divisors on curves

Let C be a curve over $\mathbb{F}_q$.

Definition 2.2 (Degree of a point)**.** Let $P \in C(\bar{\mathbb{F}}_q)$. There is a minimal extension $\mathbb{F}_{q^n}$ of $\mathbb{F}_q$ such that P is defined over. This n is defined to be the degree of P.

Exercise 7. Show that:

$$|C(\mathbb{F}_{q^n})| = \sum_{d|n} d \cdot \#\{x \in C(\bar{\mathbb{F}}_q) \mid \deg(x) = d\}.$$

Exercise 8. Find the number the of degree n points on $\mathbb{A}^1_{\mathbb{F}_q}$ (remember that on $\mathbb{A}^1$, points arise as solutions to polynomials in on variable). This leads to a version of the 'prime number theorem' for finite fields.

Definition 2.3. A *divisor* on C is a $\mathbb{Z}$-linear combination of points on the curve, i.e. something of the form:

$$\sum_{P \in C(\bar{F}_q)} n_P \, P$$

where $n_P \in \mathbb{Z}$ and all but finitely many n_P are 0.

Note that we do not insist that the points themselves be defined over $\mathbb{F}_q$ - they can be defined over an extension. The field of definition of the divisor is determined by the action of $\mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$ on it. A divisor is said to be *defined over* $\mathbb{F}_q$ or $\mathbb{F}_q$*-rational* if it is fixed by the action of $\mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$.

Example 2.4. Let $y^2 = f(x)$ be a hyperelliptic curve over $\mathbb{F}_q$. Fix $x \in \mathbb{F}_q$. Let $P_1 = (x, \sqrt{f(x)})$ and $P_2 = (x, -\sqrt{f(x)})$. Then the divisor $P_1 + P_2$ is defined over $\mathbb{F}_q$.

We will denote by $\mathrm{Div}(C)$ the group of divisors on C. Let $f \in k(C)$. Thus f has some zeros and poles. The divisor associated to f is defined as:

$$\mathrm{div}(f) := \sum_P \mathrm{ord}_P(f) \cdot P$$

where $\mathrm{ord}_P(f)$ denotes the order of f at P. The divisor of zeros of f is

$$\mathrm{div}_0(f) := \sum_{\mathrm{ord}_P(f)>0} \mathrm{ord}_P(f) \cdot P.$$

Similarly, the portion with $\mathrm{ord}_P < 0$ is called the divisor of poles and is denoted $\mathrm{div}_\infty(f)$. Let's do an example. Let C be an elliptic curve: $y^2 = x^3 + Ax + B$. Let f be the rational function x. This has two zeros P_1 and P_2 and a double pole at $\infty = [0:1:0]$. If $B \neq 0$, then P_1 and P_2 are distinct and else, not. Thus:

$$\mathrm{div}(x) = P_1 + P_2 - 2\infty.$$

A divisor D is called *principal* if there is a rational function f on C such that $D = \mathrm{div}(f)$.

Definition 2.5. Let D be a divisor defined over $\mathbb{F}_q$. The *degree* of a divisor $D = \sum n_P P$ is defined as $\deg(D) = \sum_{\text{Galois orbits}} n_P \deg(P)$.

Remark 2.6. Note that these definitions have nothing to do with the field $\mathbb{F}_q$ - you can replace this with any field you like.

Exercise 9.

1. Show that $\mathrm{Div}^0(C)$, the set of degree 0 divisors forms a subgroup of $\mathrm{Div}(C)$.
2. Show that a principal divisor has degree 0 and that $\mathrm{Prin}(C)$, the set of principal divisors on C forms a subgroup of $\mathrm{Div}^0(C)$. It is important that C is projective here.

Two divisors D and D' are linearly equivalent if there is a rational function f such that $D = D' + \mathrm{div}(f)$.

Definition 2.7. The Picard group of C is defined as:

$$\mathrm{Pic}(C) = \mathrm{Div}(C)/\mathrm{Prin}(C)$$

and the Jacobian of C is defined as:

$$(\mathrm{Pic}^0(C) :=) \, \mathrm{Jac}(C) := \mathrm{Div}^0(C)/\mathrm{Prin}(C).$$

Exercise 10. Show that for $C = \mathbb{P}^1$, the map $\mathrm{Pic}(C) \to \mathbb{Z}$ sending a divisor to its degree is an isomorphism. In other words all degree 0 divisors are principal.

Proposition 2.8. *If E is an elliptic curve* $\mathrm{Pic}^0(E) \cong E$.

The map from E to $\mathrm{Pic}^0(E)$ is given by $P \mapsto [P] - [O]$ where O is the identity element of the group law. This map is called the Abel-Jacobi map. In general, if C is a curve that has an $\mathbb{F}_q$-rational point, say O, then the Abel-Jacobi map $C \to \mathrm{Jac}(C)$ is defined by sending $P \mapsto [P] - [O]$. This map is always injective, but in the case of elliptic curves, it is also surjective. This can be proved using Riemann Roch (see Exercises, Subsection 2).

Exercise 11. (AG) Compute the Picard group of $\mathrm{Spec}\,\mathbb{Z}$.

2.1.1 The genus of a curve

A differential form on C is a $k[C]$-linear combination of elements df, with $f \in k[C]$ such that:

1. $d(f+g) = df + dg$, and $d(af) = adf$ for $a \in \mathbb{F}_q$ and $f, g \in k[C]$,
2. (Liebnitz rule) $d(fg) = fdg + gdf$, and
3. $da = 0$ for $a \in \mathbb{F}_q$.

You can make sense zeros and poles of a differential form ω (see below) and so you can associate a divisor $\operatorname{div}(\omega)$ to it. Such an ω is called holomorphic if $\operatorname{div}(\omega)$ has no poles. Let Ω_C be the space of holomorphic differentials defined on C. This is a vector space over $\mathbb{F}_q$. The dimension of this vector space is called the *genus* of the curve.

Zeros and poles of a differential form We will write the divisor associated to ω as $\sum_P \operatorname{ord}_P(\omega) \cdot P$, and define $\operatorname{ord}_P(\omega)$. Since C is a curve, around P, C can be written in terms of a single variable, t (If you have seen some algebraic geometry, this is picking a local coordinate or a uniformizer for the local ring at P. If not, you can think of this as a version of the inverse function theorem.) Write $\omega(t)$ as $f(t)dt$. Then $\operatorname{ord}_P(\omega) := \operatorname{ord}_{t=0} f(t)$.

Example 2.9. Consider the elliptic curve $E : y^2 = x^3 + Ax + B = (x - e_1)(x - e_2)(x - e_3)$ and $\omega = dx$. Let $P = (x_P, y_P)$ be a point on the elliptic curve. We want to find the uniformizer at P. If $y_P \neq 0$, then $t = x - x_p$ serves as a uniformizer. Since $\omega = dt$, $\operatorname{ord}_P(\omega) = 0$. If $P = (e_i, 0)$, then y is a uniformizer. So $(x - e_i) = y^2 u$, for some unit in the local ring at P_i and thus $dx/dy = 2yu +$ higher order terms in y. Thus $\operatorname{ord}_P(\omega) = 1$. Further dx has a pole of order 3 at ∞ since x has a pole of order 2.

Exercise 12. Show that $\omega = \frac{dx}{y}$ is a holomorphic differential on E. Further, show that E has genus 1. It is no coincidence that $\deg(\operatorname{div}\omega) = 0 = 2g - 2$.

Example 2.10. Let C be the curve:

$$y^2 = f(x)$$

for some polynomial $f(x)$ over a finite field of odd characteristic. If f has degree d, then $d = 2g + 1$ or $d = 2g + 2$, where g is the genus of the curve.

You can try to prove this using the Riemann-Hurwitz formula (♟). The formula in this case, i.e the tamely ramified case, is given by the expression in Theorem 1.1 in `https://www.staff.science.uu.nl/~oort0109/EigArt-RHurwitz-2016.pdf`. The article also explains why the expression holds in characteristic p, and what happens when a cover is wildly ramified.

Exercise 13. Show that for a hyperelliptic curve C of genus g, the differential form dx/y has degree $2g - 2$. For this, you might need to use the fact the if $\deg(f)$ is odd, then the map $C \to \mathbb{P}^1$ is ramified over $\infty \in \mathbb{P}^1$, i.e. the curve has one point at ∞. If the degree is even, it has two points at infinity.

2.1.2 Frobenius action

The Frobenius map $\operatorname{Frob}_q : (x, y) \mapsto (x^q, y^q)$ also makes sense for a higher genus curve C defined over $\mathbb{F}_q$. In fact, so does $C^{(p)}$. For instance, if C is a plane curve given by equations $\sum a_{ij} x^i y^j$, then $C^{(p)}$ is given by $\sum a_{ij}^p x^i y^j$. It follows from the way we defined the Jacobian of C, that $\operatorname{Jac}(C)$ is also defined over $\mathbb{F}_q$, and thus has a Frobenius action on it.

3 The Weil conjectures

3.1 The Tate module of the Jacobian

The Jacobian of a curve C is an algebraic variety of dimension g, and comes equipped with a group structure (you can see this from the definition). It is also complete and connected, which means it's an *abelian variety*.

You do not need to know what an abelian variety is in order to understand this section - all you need to keep in mind really, is that they come equipped with a group structure. In particular, we can define an isogeny as in the elliptic curve case. An isogeny between two abelian varieties A and B is surjective map (on $\bar{\mathbb{F}}_q$ points) that has finite kernel. An example of an isogeny is the multiplication by n map:

$$\begin{aligned}[n] : \mathrm{Jac}(C) &\to \mathrm{Jac}(C)\\ D &\mapsto n \cdot D.\end{aligned}$$

As before, we can talk about the n torsion of the Jacobian.

Fact 3.1. If $(n, p) = 1$, then:

$$\mathrm{Jac}(C)[n](\bar{\mathbb{F}}_q) \cong (\mathbb{Z}/n\mathbb{Z})^{2g}.$$

For a prime $\ell \neq p$, define:

$$T_\ell(C) := T_\ell(\mathrm{Jac}(C)) := \varprojlim \mathrm{Jac}(C)[\ell^n](\bar{\mathbb{F}}_q)$$

where the maps are given by multiplication by ℓ. Note that $T_\ell(C) \cong \mathbb{Z}_\ell^{2g}$. Just like the elliptic curve case, the Tate module of the Jacobian of a curve also has a Frobenius action on it, induced by the action of Frobenius on the curve. This is a $2g \times 2g$ matrix.

Notation 3.2. We will let $P_{C,q}(x)$ denote the characteristic polynomial of Frob_q acting on $T_\ell(C)$. This is a monic polynomial defined over $\mathbb{Z}$ of degree $2g$. Write:

$$P_{C,q}(x) = \prod_{i=1}^{2g}(x - \alpha_i),$$

where α_i are the Frobenius eigenvalues.

Note that the size of $\mathrm{Jac}(C)(\mathbb{F}_q)$ is given by the degree of the map $(\mathrm{Frob}_q - id)$ (equivalently, the size of the kernel). Thus, $|\mathrm{Jac}(C)(\mathbb{F}_q)| = P_{C,q}(1)$.

Exercise 14. Let C be the curve $y^2 = x^6 + 2x^2 - x + 1$ over $\mathbb{F}_5$. Use Sage or Magma to calculate $P_{C,5}(x)$ and its eigenvalues. What happens if you define C over higher powers of 5 and calculate $P_{C,5^n}(x)$?

3.2 The Zeta Function of a curve

Let C be a curve of genus g over $\mathbb{F}_q$. As we have seen before, for any extension $\mathbb{F}_{q^n}$ of $\mathbb{F}_q$, you can consider $C(\mathbb{F}_{q^n})$, i.e. the points whose coordinates satisfy $x_i^{q^n} = x_i$. We want to take these and put them into a generating series. This is called the Zeta function $Z(C, T)$ of the curve.

$$Z(C, T) = \exp\left(\sum_n |C(\mathbb{F}_{q^n})|T^n/n\right).$$

Example 3.3. Let $C = \mathbb{A}^1$ (this is not projective, but the definition still makes sense. Then $|C(\mathbb{F}_{q^n})| = q^n$. So:

$$Z(\mathbb{A}^1, T) = \exp\left(\sum_n (qT)^n/n\right) = \exp(-\log(1 - qT)) = \frac{1}{1 - qT}.$$

Example 3.4. Let $C = \mathbb{P}^1$. Then

$$Z(\mathbb{P}^1, T) = \exp\left(\sum_n (qT)^n/n + \sum_n T^n/n\right) = \frac{1}{(1 - T)(1 - qT)}.$$

Exercise 15. For a curve C, one can define a different zeta function by:

$$\zeta_C(s) = \prod_{x \in C}(1 - q^{-\deg(x)s})^{-1}$$

where $\deg(x)$ is the degree of the extension over which the point $x \in C$ is defined. Show that $Z(C, q^{-s}) = \zeta_C(s)$. Use this to show that $\zeta_{\mathbb{A}^1}(s)$ has a simple pole at $s = 1$.

This is the "function field" version of the Riemann zeta function, which can be written as:

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

3.2.1 Statement of the Weil Conjectures

The Weil conjectures are a collection of statements about (smooth, projective, geometrically irreducible) varieties over $\mathbb{F}_q$. The special case for curves was conjectured by Artin in the '20s and proved by Weil in the '40s. Rationality of the zeta function in the general case was proved by Dwork in the '60s. The Riemann Hypothesis was proved by Deligne in the '70s, and the process led to the revolutionary development of new cohomology theories by Artin, Grothendieck and Verdier. In this section, I will only state the version for curves.

Theorem 3.5 (Weil conjectures for curves)**.** *Let C be a smooth projective curve over $\mathbb{F}_q$.*

1. *(Rationality)*
$$Z(C,T) = \frac{\prod_{i=1}^{2g}(1-\alpha_i T)}{(1-T)(1-qT)}$$
where the α_i's are the eigenvalues of Frobenius.

2. *(Functional equation)*
$$Z(C,(qT)^{-1}) = q^{1-g}T^{2-2g}Z(C,T).$$

3. *(Riemann Hypothesis) $|\alpha_i| = q^{1/2}$, where $|\cdot|$ denotes the complex norm.*

The numerator of $Z(C,T)$ is often denoted called the L-polynomial of C, denoted $L(C,T)$. In our notation, $L(C,T) = T^{2g}P_{C,q}(\frac{1}{T})$. Since $P_{C,q}(x)$ is defined over $\mathbb{Z}$, its zeros must appear in conjugate pairs. Part (3) of Theorem 3.5 implies that $\alpha\bar{\alpha} = q$ for α a zero of $P_{C,q}(x)$. Further, write:

$$P_{C,q}(x) = a_{2g} + a_{2g-1}x + \ldots a_1 x^{2g-1} + x^{2g}.$$

It follows that $a_{2g} = q^g$.

From Exercise 15 we have that $\zeta_C(s) = Z(C, q^{-s})$. Part (3) asserts that the zeros of $\zeta_C(s)$ lie on $s = \frac{1}{2}$, thus justifying the name 'Riemann Hypothesis.'

Exercise 16. Let C be the curve $y^2 = x^6 + 2x^2 - x + 1$ over $\mathbb{F}_5$. Calculate the number of points $C(\mathbb{F}_{5^n})$ for a few n (you can use a computer for this part) and use this to calculate the Frobenius polynomial $P_{C,q}(x)$ by hand. You might find it useful to keep track of how many n you need to determine $P_{C,q}(x)$. Hint: use the functional equation to reduce the number of calculations you need.

Exercise 17. Use the zeta function of a curve $C/\mathbb{F}_q$ to show that:

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

Corollary 3.6 (Hasse-Weil bound)**.** *If C is a smooth projective curve of genus g over $\mathbb{F}_q$, $||C(\mathbb{F}_q)| - q - 1| \leq 2g\sqrt{q}$.*

Proof. This follows quite easily from the Weil conjectures. Using the above exercise, we have that: $C(\mathbb{F}_{q^n}) - q^n - 1 = \sum_{i=1}^{2g} \alpha_i^n$. Further, by the Riemann Hypothesis,

$$\left|\sum_{i=1}^{2g} \alpha_i^n\right| \leq 2g\sqrt{q^n},$$

which gives us what we want. □

Exercise 18 (Hasse-Weil-Serre bound)**.** Let $\{\alpha_1, \dots \alpha_g, \bar{\alpha}_1 \dots \bar{\alpha}_g\}$ be the eigenvalues of Frobenius. Set $x_i = \lfloor 2\sqrt{q} \rfloor + 1 + \alpha_i + \bar{\alpha}_i$, and show that x_i is totally real. Thus $\prod_{i=1}^{g} x_i \geq 1$. Use this to show that:

$$|C(\mathbb{F}_q) - q - 1| \leq \lfloor 2\sqrt{q} \rfloor g.$$

Exercise 19 (Ihara's bound)**.** For a curve C we have

$$|C(\mathbb{F}_q)| \leq |C(\mathbb{F}_{q^2})| = q^2 + 1 - \sum_{i}^{g} (\alpha_i^2 + \bar{\alpha}_i^2) = q^2 + 1 + 2gq - \sum_{i}^{g} t_i^2$$

where $t_i = \alpha_i + \bar{\alpha}_i$. Use the Cauchy-Schwartz inequality to show that:

$$|C(\mathbb{F}_q)| \leq q + 1 - g \left(\sqrt{2q + \frac{1}{4} + \frac{q^2 - q}{g}} - \frac{1}{2} \right).$$

When is this bound better than the Weil bound?

4 p-torsion in characteristic p

Recall from Galois theory that a polynomial $f(x) \in k[x]$ is *separable* if it has distinct roots over the algebraic closure $\bar{k}$. So, for instance: $x^p - 1$ is not separable over a field of characteristic p. An extension of fields K'/K is called separable if the minimal polynomial of every $\alpha \in K'$ is separable. A map of two curves $C \to C'$ is called separable if the corresponding extensions of function fields is separable.

Let E be an elliptic curve over $\mathbb{F}_q$. The map

$$F := \mathrm{Frob}_p : E \to E^{(p)}; \quad (x, y) \mapsto (x^p, y^p)$$

is a purely inseparable map of degree p. Note that the number of pre-images of a point (a, b) is exactly 1, since $x^p - a = (x - a^{1/p})^p$ and $y^p - b = (y - b^{1/p})^p$.

Exercise 20. Let $f : X \to Y$ be a map of two curves. Then f induces a map on the space of differentials given by $f^* dg = d(g \circ f)$. One way to check if a map is purely inseparable is to check whether its action on differentials is identically 0. This is true even for higher dimensional varieties. Show that the Frobenius map F induces the zero map on differentials.

Fact 4.1. The multiplication by p map on abelian varieties over $\mathbb{F}_q$ factors through F. Since we are only interested in Jacobians of curves (recall that an elliptic curve is isomorphic to its own Jacobian), this is equivalent to saying that there is an isogeny $V : \mathrm{Jac}(C)^{(p)} \to \mathrm{Jac}(C)$ such that:

$$V \circ F = [p].$$

Further, F and V are both of degree p^g. For elliptic curves, this is just the dual isogeny.

In particular, the following is true:

Corollary 4.2. *Let $E/\mathbb{F}_q$ be an elliptic curve. Then:*

$$E[p](\bar{\mathbb{F}}_q) \cong \begin{cases} \mathbb{Z}/p\mathbb{Z} \\ 0. \end{cases}$$

The first case is called ordinary and the second is called supersingular.

Idea of proof: Since $V \circ F = [p]$, we have that $\mathrm{Ker}(F) \subset E[p]$. Since F is purely inseparable of degree p, $\mathrm{Ker}(F)(\bar{\mathbb{F}}_q)$ is trivial. Thus the size of $E[p](\bar{\mathbb{F}}_q)$ depends on whether V is separable or inseparable.

Exercise 21. 1. Let $C \to C'$ be a purely inseparable degree p map of curves over $k = \mathbb{F}_q$. Show that C' must be isomorphic to $C^{(p)}$. Hint: Show that the subextension $k(C')$ of $k(C)$ contains all p-th powers of functions.

2. If $E/\mathbb{F}_q$ is supersingular, show that $j(E) \in \mathbb{F}_{p^2}$. *Hint:* Show using the above exercise that V must factor through the Frobenius map on $E^{(p)}$, and therefore $E^{(p^2)}$ must be isomorphic to E.

3. Show that there are only finitely many isomorphism classes of elliptic curves over $\bar{\mathbb{F}}_p$ that are supersingular.

Definition 4.3. For a general curve, $\mathrm{Jac}(C)[p](\bar{\mathbb{F}}_q) \cong (\mathbb{Z}/p\mathbb{Z})^s$ where $0 \leq s \leq g$. This is because the Frobenius is always purely inseparable of degree p^g, and $\operatorname{Ker} F \subset \operatorname{Ker}[p] = \mathrm{Jac}(C)[p](\bar{\mathbb{F}}_q)$. This s is called the p-rank of the curve.

A curve with p-rank equal to g is called ordinary. The notion of supersingular is more nuanced for higher genus curves: we will talk about it once we have defined Newton Polygons. There are also other invariants one can use to study the p-torsion of higher dimensional Jacobians in characteristic p. ( here is a short survey paper, but this requires a lot more background in algebraic geometry. Maybe you want to store it in a mind palace for now: `https://arxiv.org/pdf/math/0609658.pdf`).

4.0.1 Ordinarity for Elliptic Curves

Let E be an elliptic curve over $\mathbb{F}_p$. Consider F and V as endomorphisms on the Tate module $T_\ell(E)$. Since we the Tate module is 2-dimensional and $V \circ F = [p]$, we must have (from the characteristic polynomial of F) that:

$$[a_p] = F + V.$$

Now, if you consider the differential: $\omega = \frac{dx}{2y}$, then $F^*(\omega) = 0$ since the Frobenius map is purely inseparable. Thus,

$$V^*(\omega) = a_p\omega.$$

To determine if an elliptic curve is supersingular, by the proof of Corollary 4.2, we need only determine if V is inseparable. Thus E is supersingular if and only if $a_p \equiv 0 \mod p$. Similarly, if we started with an elliptic curve E' over $\mathbb{F}_q$, with q a power of p, E' is supersingular if and only if $a_q(E') \equiv 0 \mod p$.

Exercise 22. Check if the following curve is ordinary or supersingular over $\mathbb{F}_7$:

$$E : y^2 = x^3 + 2x + 3.$$

4.0.2 Computing the Hasse Invariant

In this section, we will learn a quick way of testing whether an elliptic curve is ordinary or supersingular. Let $E : y^2 = f(x)$ be an elliptic curve over $\mathbb{F}_p$. For $a \in \mathbb{F}_p$, $a^{(p-1)/2} = \left(\frac{a}{p}\right)$. Thus $f(x)^{(p-1)/2} = a(x)$ (as defined in Lecture 1). Therefore, modulo p we have:

$$|E(\mathbb{F}_p)| = p + 1 \sum_{x \in \mathbb{F}_p} a(x) = p + 1 + \sum_{x \in \mathbb{F}_p} (f(x))^{(p-1)/2} = p + 1 + \sum_{x \in \mathbb{F}_p} \sum_{i=1}^{3(p-1)/2} c_i x^i.$$

Now,

$$\sum_{x \in \mathbb{F}_p} \sum_{i=1}^{3(p-1)/2} c_i x^i = \sum_{i=1}^{3(p-1)/2} c_i \sum_{x \in \mathbb{F}_p} x^i.$$

Exercise 23. Show that in the above sum $\sum_{x \in \mathbb{F}_p} x^i$ is only non zero when $i = p - 1$. Also calculate the value of $\sum_{x \in \mathbb{F}_p} x^{p-1}$.

Thus, $|E(\mathbb{F}_p)| \equiv 1 - c_{p-1} \mod p$. So we have $a_p \equiv c_{p-1} \mod p$. Since $a_p \equiv 0 \iff E$ is supersingular, the constant c_{p-1} (called the Hasse invariant) serves as a test for supersingularity. One can also use c_{p-1} as a test for supersingularity if E is defined over $\mathbb{F}_q$ (see exercises).

Remark 4.4. For any $r \geq 1$, one may consider the torsion subgroups $E[p^r]$. If E is ordinary, then $E[p^r] \cong \mathbb{Z}/p^r\mathbb{Z}$ and if E is supersingular, then $E[p^r] = 0$ for all r. This happens because the map $[p^r]$ factors as $V^r \circ F^r$. A similar property is true for higher genus curves as well.

4.1 Newton Polygons

Newton Polygons are combinatorial objects that give us arithmetic information about varieties. In this section, we focus on Newton Polygons coming from Frobenius polynomials of curves, but the construction makes sense for any polynomial.

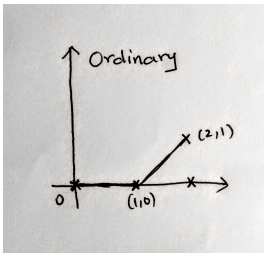
Let C be a curve over $\mathbb{F}_p$ and let $P_{C,p}(t)$ denote the characteristic polynomial of Frob_p. Write $P_{C,p}(t) = a_{2g} + a_{2g-1}t + \ldots a_0 t^{2g}$. Consider the following set:

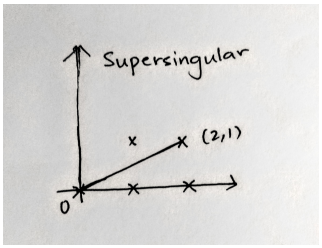
$$S = \{(i, \nu_p(a_i) \mid 0 \leq i \leq 2g, a_i \neq 0\}$$

The Newton Polygon of C (technically $\text{Jac}(C)$) is defined as the lower convex hull of this set. If C is defined over $\mathbb{F}_q$, where $q = p^r$, then the valuations of the a_i's are normalized so as to have the rightmost point be $(2g, g)$.

4.1.1 Examples

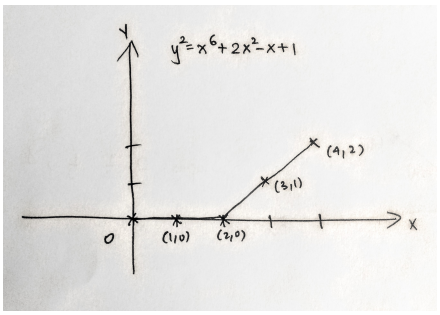
Elliptic curves:

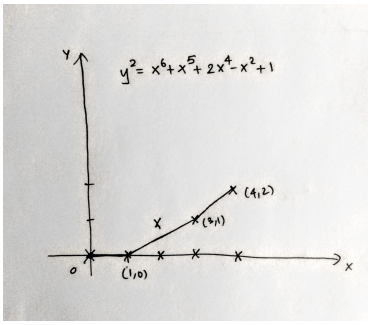




(Ignore the stray point in the second picture)
The slopes of the Newton Polygon can give us arithmetic information about the curve. For instance, an ordinary elliptic curve always has slopes $[0, 1]$, while a supersingular elliptic curve has slopes $[1/2, 1/2]$.

Genus 2 curves:





Curve on the left: $y^2 = x^6 + 2x^2 - x + 1$ over $\mathbb{F}_5$.
Numerator of zeta function: $25T^4 + 10T^3 + 6T^2 + 2T + 1$.
Newton slopes: $[0, 0, 1, 1]$.

Curve on the right: $y^2 = x^6 + x^5 + 2x^4 - x^2 + 1$ over $\mathbb{F}_5$.
Numerator of zeta function: $25T^4 + 15T^3 + 5T^2 + 3T + 1$
Newton slopes: $[0, 1/2, 1/2, 1]$.

Note that as the genus increases, the number of possibilities for the Newton Polygon increases.

Definition 4.5. A curve C (or its Jacobian) is called *supersingular* if all the slopes of its Newton Polygon are equal to $1/2$.

Some properties of the Newton Polygon

1. A Newton Polygon always starts at $(0, 0)$ and ends at $(2g, g)$ (follows from the Weil conjectures).
2. Symmetry: there are as many segments of slope λ, as there are of slope $1 - \lambda$.
3. The p-rank of the curve is the number of slope zero segments of the Newton Polygon.

5 Exercises

These exercises are in addition to the ones listed in the lectures. You are not expected to do all of them. The ones that are more geometric in nature (not necessarily requiring background in algebraic geometry) are marked with an (ag).

5.1 Lecture 1

1. (ag) Let $f(X_0, X_1 \dots X_n)$ be a homogeneous polynomial. Then the variety in $\mathbb{P}^n$ cut out by $f = 0$ is smooth if f and $\frac{\partial f}{\partial X_i}$ do not all vanish simultaneously (there is a general version for multiple polynomials as well). Show that the curve:

$$Y^2 Z = (X - e_1 Z)(X - e_2 Z)(X - e_3 Z)$$

   is smooth if and only if the e_i's are distinct.

2. (ag) Let $C \xrightarrow{f} C'$ be a surjective map of curves over an algebraically closed field k. Let $k(C') \hookrightarrow k(C)$ be the corresponding extension of function fields. The notion of a 'prime' in a function field is that of a point on the curve (if k is not algebraically closed, this is replaced by a certain collection of points). Let $P \in C$ and $P' \in f^{-1}(P)$. One can localize $k[C]$ and $k[C']$ at P and P' respectively. We will often find it useful to study the extension of local fields $k(C')_{P'}/k(C)_P$.

   Fact 5.1. If C is a smooth curve, then the (completed) local ring at a point $P \in C$ is of the form $k[[t]]$, where t is a generator of the maximal ideal at P. The local field $k(C)_P \cong k((t))$ comes equipped with a valuation ord_P. In particular $\mathrm{ord}_P(t) = 1$.

   Now, let $C = E$ an elliptic curve given by $y^2 = (x - e_1)(x - e_2)(x - e_3)$, $C' = \mathbb{P}^1$ and $f : (x, y) \mapsto [x : 1]$.

   (a) Describe the extension of function fields $k(\mathbb{P}^1) \hookrightarrow k(E)$.

   (b) Show that this extension is ramified at points where $f(x) = 0$ and at ∞ by calculating the uniformizers of the local extensions.

3. (ag) Let E be an elliptic curve over $\mathbb{F}_q$. Show that $\mathrm{Frob}_p : E \to E^{(p)}$ has degree p. *Hint:* Show that $\mathrm{Frob}_p^* k(E^{(p)}) = (k(E))^p$.

4. The group law on an elliptic curve is determined as follows: Let P and Q be two $\bar{\mathbb{F}}_q$ points on $E : y^2 = x^3 + Ax + B$. A line passing through P and Q necessarily intersects E in a third point, say R. We then demand that $P + Q + R = 0$. If $P = Q$, then we take the tangent line at P. Show that any 2-torsion point on E must have y-coordinate 0.

5. Let p be an odd prime. Let $E/\mathbb{F}_p$ be given by $y^2 = x^3 + Ax^2 + x$, such that $A \neq \pm 2$ in $\mathbb{F}_p$. If $\left(\frac{A^2-4}{p}\right) = 1$, then show that E has full 2-torsion.

6. Let $p \equiv 2 \mod 3$. Show that the elliptic curve $E : y^2 = x^3 + B$, $B \in \mathbb{F}_p^*$ has $p+1$ points over $\mathbb{F}_p$. *Hint:* note that if $p \equiv 2 \mod 3$, then $\mathbb{F}_p$ does not have any cube roots of unity.

7. A quadratic twist of an elliptic curve E is a curve E' defined over the same field such that E and E' are not isomorphic over the base field, but are isomorphic after a quadratic extension. Let p be an odd prime. For what values of a are $y^2 = x^3 + Ax + B$ and $ay^2 = x^3 + Ax + B$ non-trivial quadratic twists of each other?

8. Let $\alpha : E \to E'$ and $\beta : E \to E$ be two isogenies over $\mathbb{F}_q$ such that $\mathrm{Ker}(\alpha) \subset \mathrm{Ker}(\beta)$. Show that there exists an isogeny $\gamma : E' \to E$ such that $\beta = \gamma \circ \alpha$.

9. Let $\phi : E \to E'$ be an isogeny of degree n. Then there is an isogeny $\hat{\phi} : E' \to E$ such that $\hat{\phi} \circ \phi = [n]$. If n is coprime to p, then you can prove this directly from the above exercise, but this is true more generally. This is called the *dual isogeny*.

   Show that if E and E' are two isogenous elliptic curves over $\mathbb{F}_q$, then $|E(\mathbb{F}_q)| = |E'(\mathbb{F}_q)|$. (In fact the converse is also true, and is a consequence of Tate's isogeny theorem).

5.1.1 Computational questions

1. Familiarize yourself with the following commands and constructions in Sage or Magma:
   - Commands for creating a finite field $\mathbb{F}_p$ or $\mathbb{F}_q$.
   - Elliptic Curve constructors - both long and short Weierstrass form.
   - Point search commands: rational_points() or cardinality() in Sage or RationalPoints() or PointSearch() in Magma.
   - Trace of Frobenius and Frobenius polynomial commands.
2. Let E be the elliptic curve defined by $y^2 + y = x^3 - x$ over $\mathbb{F}_{11}$. Find the number of $\mathbb{F}_{11}$-rational points on E. Use this to compute the trace of Frobenius on E.
3. Calculate the number of points on a few (this will depend on how large $\mathbb{F}_q$ is) elliptic curves over $\mathbb{F}_q$ and check how often these curves are maximal, i.e. $|E(\mathbb{F}_q)|$ achieves the Hasse-Weil bound of $q + 1 + 2\sqrt{q}$.

5.2 Lecture 2

1. Calculate the number of $\mathbb{F}_p$ rational points on the curve defined by $x^2 + y^2 = 1$ in $\mathbb{A}^2$. *Hint:* the homogenized version of this curve $x^2 + y^2 = z^2$ has 1 or 2 points at ∞ depending on $p \mod 4$.
2. Let C be the curve given by $x^3y + y^3z + z^3x = 0$ in $\mathbb{P}^2$ over $\mathbb{F}_2$. Compute $|C(\mathbb{F}_{2^m})|$ for $1 \leq m \leq 3$.
3. The degree-genus formula for a smooth plane curve states that:
$$g = \frac{1}{2}(d-1)(d-2).$$
   What is the genus of the curve in exercise 2?
4. Let p be an odd prime and let C be the curve defined over $\mathbb{F}_p^2$ by the equation:
$$y^p + y = x^{p+1}.$$
   (a) Show that this curve has a unique point at ∞.
   (b) If z_1, $z_2 \in \mathbb{F}_{p^2}$ such that $z_1^p + z_1 = a \in \mathbb{F}_p$ and $z_2^p + z_2 = 0$, then show that $(z_1 + z_2)^p + (z_1 + z_2) = a$.

(c) Show that $|C(\mathbb{F}_{p^2})| = 1 + p^3$, and in particular $|C(\mathbb{F}_{p^2})| = 1 + p^2 + 2gp$. Later, we can compare this with what we learn in Lecture 3.

5. (ag) A divisor $D = \sum n_P P$ on a curve C is said to be effective (denoted $D \geq 0$) if $n_P \geq 0$ for each P. One can define:
$$\mathcal{L}(D) = \{f \in k(C) \mid \mathrm{div}(f) + D \geq 0\}.$$
This is a vector space over the ground field. Let $\ell(D) := \dim \mathcal{L}(D)$. Any variety comes equipped with a special divisor, called the canonical divisor, K. For a curve, we can calculate this by taking $\omega \in \Omega_C$ and let $K = \mathrm{div}(\omega)$. (It turns out that $\ell(K)$ is an equivalent way of defining genus). The Riemann-Roch theorem states that for any divisor D:
$$\ell(D) - \ell(K - D) = \deg(D) - g + 1.$$
   (a) Show that if D has some coefficient that is negative, then $\ell(D) = 0$ (this has nothing to do with RR).
   (b) Show that $\deg(K) = 2g - 2$.
   (c) Prove that $\ell(D) \leq \deg(D) - g + 1$ and that if $\deg(D) > 2g - 2$, then $\ell(D) = \deg(D) - g + 1$.

   Philosophy: Riemann-Roch is a hammer. Whenever you want to find functions or effective divisors, use the hammer.

6. (ag) This exercise shows that the Abel-Jacobi map $E \to \mathrm{Pic}^0(E)$ sending $P \mapsto [P] - [O]$ is surjective. Let $D \in \mathrm{Pic}^0(E)$. Use Riemann Roch to show that $\mathcal{L}(D + [O])$ is non empty. In particular, there is an effective divisor E such that $E \sim D + [O]$. Show that this divisor must have degree 1.

7. Show that for a curve of higher genus too, the Frobenius map $C \to C^{(p)}$ has degree p (The proof is the same as as the case of elliptic curves).

8. Let C be the hyperelliptic curve given by $y^2 = -(x^3 - x)^2 - 1$ defined over $\mathbb{F}_3$.
   (a) Show that C has no $\mathbb{F}_3$ points.
   (b) Show that C has a $\mathbb{F}_3$-rational divisor degree 1 as follows. Consider the points $(0, \alpha_1), (0, \alpha_2)$ in $C(\mathbb{F}_9)$. Show that the divisor $(0, \alpha_1) + (0, \alpha_2)$ is defined over $\mathbb{F}_3$.
   (c) Similarly, show that if $\beta_1, \beta_2, \beta_3$ are roots of the polynomial $t^3 - t = -1$, then the divisor $(\beta_1, 1) + (\beta_2, 1) + (\beta_3, 1)$ is defined over $\mathbb{F}_3$.
   (d) Write down an $\mathbb{F}_3$-rational divisor of degree 1 on C.

5.2.1 Computational questions

1. Commands to know: curve constructors, hyperelliptic curve constructors, Jacobians, finding rational points.

2. Calculate the number of $\mathbb{F}_9$-rational points on the curve $C : y^2 = x^8 + x^5 + 3x^3 + 1$ over $\mathbb{F}_9$. Calculate the Frobenius polynomial of C. What is its degree?

3. Implement the following Sage code and interpret your output.

```
k = GF(5);
R.<x>=PolynomialRing(k);
C=HyperellipticCurve(x^6 + x - 1);
J=C.jacobian();
X=J(k);
A=C.rational_points();
X(A[1])-X(A[2]);
```

If you want, you can also implement this in Magma (you don't need to create the Jacobian in Magma, you can directly use the Divisor() function). What would happen if you tried to calculate A[1]-A[2] directly?

4. In the above example, calculate the number of $\mathbb{F}_5$ points on the Jacobian (you might want to do this after Lecture 3).

5.3 Lecture 3

1. Consider the curve [Exercises:Lecture 2, Exercise 2] given by $C : x^3y + y^3z + z^3x = 0$ over $\mathbb{F}_2$. Show that $Z(C, T)$ is given by:
$$\frac{1 + 5t^3 + 8t^6}{(1 - T)(1 - qT)}$$

2. How many $\mathbb{F}_{q^r}$ points does $\mathbb{P}^n$ have? Use this to compute $Z(\mathbb{P}^n_{/\mathbb{F}_q}, T)$ (defined analogously).

3. Let $\{\alpha_1, \alpha_2, \ldots \alpha_{2g}\}$ denote the eigenvalues of Frobenius. Show that this set is fixed by the permutation $\alpha \mapsto q/\alpha$.

4. Let C be the hyperelliptic curve over $\mathbb{F}_7$ defined by:
$$y^2 = x(x - 1)(x - 2)(x - 5)(x - 6)$$
   (a) What is the genus of this curve?
   (b) Show that every point of the form $(a, 0)$ is a 2-torsion of the Jacobian of this curve.
   (c) Find a presentation for $\mathrm{Jac}(C)[2]$, i.e. find generators and relations, and show that $\mathrm{Jac}(C)[2] \cong (\mathbb{Z}/2\mathbb{Z})^{2g}$.
   (d) What is the matrix of Frobenius on the mod 2 Tate module of this curve?

5. Let C be the curve $x^3 + y^3 + z^3 = 0$ over $\mathbb{F}_p$ where $p \equiv 2 \mod 3$. Show that
$$Z(C, T) = \frac{1 + pT^2}{(1 - T)(1 - pT)}.$$
   Hint: for the affine part $x^3 + y^3 = -1$, notice that the number of $\mathbb{F}_p$ points is:
$$\sum_{a+b=-1} N(x^3 = a)N(y^3 = b)$$
   where $N(x^3 = a)$ is the number of solutions to $x^3 = a$ in $\mathbb{F}_p$, etc.

5.3.1 Computational questions

1. Functions to know: finding Frobenius polynomial, zeta function, L polynomial.

2. The curve in [Exercises:Lecture 2, Exercise 4] is an example of a *maximal curve* over $\mathbb{F}_{p^2}$, i.e. a curve with largest number of points possible. People who work in coding theory like maximal curves because they have lots of points (see for e.g. `https://www.math.colostate.edu/~pries/costaricalectures.pdf`). How many points does C have over $\mathbb{F}_{p^n}$ for higher n? Is it still maximal?

3. Consider the *superelliptic curve* given by:
$$y^3 = x^6 + 2x^2 + x + 1$$
   over $\mathbb{F}_7$. Compute the genus of this curve. You can try to do this by hand using the Riemann-Hurwitz formula and then check it with a computer. Sage uses the command CyclicCover() to construct such curves. Calculate the characteristic polynomial of Frobenius on this curve.

5.4 Lecture 4

1. Classify the following elliptic curves as ordinary or supersingular over $\mathbb{F}_5$:
   (a) $y^2 = x^3 + x + 1$,
   (b) $y^2 = x^3 + 1$.
2. Let $q = p^r$. This exercise walks you through showing that if E is defined over $\mathbb{F}_q$ for q a power of p, then one can check whether E is supersingular by computing c_{p-1} from Lecture 4.
   (a) Let c_{q-1} denote the coefficient of x^{q-1} in $f(x)^{(q-1)/2}$ and let c_{p-1} denote the coefficient of x^{p-1} in $f(x)^{(p-1)/2}$.
   (b) Notice that $p^{r+1} - 1 = p^r(p-1) + (p^r - 1)$.
   (c) Show that $c_{p^{r+1}-1} = c_{p^r-1}(c_{p-1})^{p^r}$.
   (d) Use induction to show that $c_{q-1} \equiv 0 \mod p \iff c_{p-1} \equiv 0 \mod p$
3. Let E be an ordinary elliptic curve over $\mathbb{F}_q$ with $q = p^n$. Let α be a root of the characteristic polynomial $P_{E,q}(x) \in \mathbb{Z}[x]$. Show that $\alpha \notin \mathbb{Q}$.
4. Draw the Newton polygon of the curve $x^3y + y^3z + z^3x = 0$ over $\mathbb{F}_2$. What is the p-rank of this curve?
5. Let C be the curve $y^2 = x^6 + x^3 + 2x^2 + x + 3 =: f(x)$ over $\mathbb{F}_7$. Write $f(x)^{(p-1)/2}$ as $\sum_m c_m x^m$. Compute the matrix: $B_{ij} = (c_{ip-j})$. This is called the Cartier-Manin matrix of C. C is ordinary if and only if this matrix has full rank. Use this to check if C is ordinary.

5.4.1 Computational questions

1. Functions to know: p-rank, is_ordinary, Np() (number of points mod p), NewtonPolygon().
2. Let E be the elliptic curve $y^2 = x^3 - x$ over $\mathbb{Q}$. Let E_p denote the reduction of E modulo p. E_p is not always an elliptic curve (it fails the smoothness criterion for certain p - here the only such prime is 2). For a bound B, how many odd $p < B$ satisfy the condition that E_p is supersingular? Compute this number for some values of B and make a conjecture about how it grows.
3. Run the same computation for $E : y^2 = x^3 + 2x + 1$. Is there any difference in the pattern from the above problem?

   The elliptic curve in the previous problem has j-invariant 1728. All elliptic curves come equipped with the automorphism $(x, y) \mapsto (x, -y)$. The elliptic curve $y^2 = x^3 - x$ has an extra automorphism, $(x, y) \mapsto (-x, iy)$. This is an example of an elliptic curve with complex multiplication (CM). Such curves behave significantly differently than curves without CM. For more on this see Chapter II of 'Advanced Topics in the Arithmetic of Elliptic Curves' by Joseph Silverman ().
4. Run the following Sage code and use it to calculate the p-rank of the given curve.

```
k=GF(7)
P.<x>=PolynomialRing(k)
C=HyperellipticCurve(x^6 + x^3 + 2*x^2 + x + 3);
C.frobenius_polynomial()
from sage.geometry.newton_polygon import NewtonPolygon
NP = NewtonPolygon([ (0,0), (1,0),(2,0),(3,1) ,(4,2) ])
polygon = NP.plot()
polygon
```

5. Plot the Newton Polygon of the curve: $x^3y + y^3z + z^3x$ over $\mathbb{F}_2$.
6. Write a script to plot the Newton Polygon of a genus 3 hyperelliptic curve.

6 References

A lot of this material can be found in Joseph Silverman's book: 'Arithmetic of Elliptic Curves.' For a comprehensive resource on abelian varieties, see Milne's notes on Abelian Varieties: `https://www.jmilne.org/math/CourseNotes/AV.pdf`. For an exposition on the Weil Conjectures, see Section 1 of: `https://arxiv.org/pdf/1807.10812.pdf`, a survey paper by Evgeny Goncharov. If you are interested in the proof, you can look up course notes from an earlier CTNT summer school: `https://ctnt-summer.math.uconn.edu/wp-content/uploads/sites/1632/2016/02/lecture-notes.pdf` taught by Bin Zhao.

If you are looking to dive into this material in the future, Richard Griffon taught a great course on Curves over finite fields, which can be found here: `http://math.richardgriffon.me/CFF1617.html`.