FULTON'S TRACE FORMULA AND ELLIPTIC CURVES OVER FINITE FIELDS

YUCHEN CHEN

Abstract. An important, but difficult question, is: how can we count the rational points of varieties over finite fields? This paper begins with an exposition on Fulton's trace formula which gives a partial answer to this question. We then turn to an application on elliptic curves. In doing so, we will investigate a fascinating connection between $\mathbb{F}_p$-points of elliptic curves and the Picard-Fuchs differential equation.

Contents

1. Introduction

This paper focuses on varieties over finite fields. If we have a variety X over a finite field $\mathbb{F}_q$, a natural question to ask is what is the cardinality of the $\mathbb{F}_q$- points, $|X(\mathbb{F}_q)|$? For instance, the count of $\mathbb{F}_q$-points of elliptic curves has important applications in cryptography and number theory. Unfortunately, it is difficult to answer this question in general.

A formula due to Fulton [Ful78], gives a partial answer in that it allows us to count $\mathbb{F}_q$-points mod p, where p is the characteristic of $\mathbb{F}_q$.

Date: August 29, 2020.

Theorem 1.1. *(Fulton) Let X be a projective scheme over $\mathbb{F}_q$ a field of characteristic p. Then,*

$$|X(\mathbb{F}_q)| = \sum_{i=0}^{dimX} (-1)^i \operatorname{tr}(F|H^i(X, \mathcal{O}_X)) \pmod{p}.$$

The idea behind this formula is to compute the fixed points of the $q-$Frobenius action on X. It is an algebraic analogue to the Lefschetz fixed point formula in topology.

This paper will be split into two sections. The first section will be dedicated to deriving Fulton's trace formula. This will involve looking at F-modules, which are coherent sheaves with Frobenius actions, along with some K_0-Theory, in particular Grothendieck groups of F-modules. We start by defining these objects and their properties. Next, we will prove a key theorem, a localization theorem. With these tools, Fulton's trace formula will follow fairly easily. We then end with a few applications to classical problems, the Chevalley-Warning theorem and the number of $\mathbb{F}_q$-points of hypersurfaces.

In the second section, we will shift our focus to elliptic curves over finite fields. This section will be centered around two computations. The first computation will be of the number of rational points of elliptic curves over finite fields mod p.

For the second computation, we will consider the Legendre family of elliptic curves over $\mathbb{C}$, parameterized over $\mathbb{P}^1 \setminus \{0, 1, \infty\}$. Here, elliptic curves have two fundamental periods relating to their identification as complex tori. We will see that these periods satisfy a differential equation in terms of the parameter called the Picard-Fuchs equation. Moreover, we will compute the solutions to this differential equation.

Unexpectedly, it turns out that an invariant determining the number of $\mathbb{F}_p$-points of elliptic curves mod p is a solution to the Picard-Fuchs equation. It is strange that the Picard-Fuchs equation derived from the analytic structure of an elliptic curve encodes arithmetic information as well. Fulton's trace formula will be used to reconcile why these two distinct computations coincide. This beautiful relationship will follow from the connection between cohomology on the structure sheaf and cohomology on the cotangent sheaf through Serre duality.

This paper will assume the basics of scheme theory as in chapter two of [Har77]. We will also need to use coherent cohomology as in chapter three of [Har77]. The most important topics are computations using Cech cohomology, specifically the computation of cohomology of projective space, the construction of higher direct images and Serre duality for curves.

2. Fulton's Trace Formula

In this section, we will prove Fulton's trace formula which is a fixed point formula of Frobenius actions on coherent cohomology. As a result, we will get a formula for the number of $\mathbb{F}_q$-points of a variety. We will primarly follow [Mus11]. We begin this exposition by discussing Frobenius actions on schemes.

2.1. The Category of F-modules.

Let X be a scheme over the finite field $\mathbb{F}_q$ of characteristic p. That is, we have a structure morphism $X \to \operatorname{Spec} \mathbb{F}_q$. For each section over an open U, this induces a morphism $\mathbb{F}_q \to \mathcal{O}_X(U)$ giving the local section the structure of a $\mathbb{F}_q$-vector space.

On X, we have a Frobenius endomorphism $F : X \to X$. On the topological space the map $F : X \to X$ is the identity map. The corresponding morphism of sheaves $\mathcal{O}_X \to F_*\mathcal{O}_X = \mathcal{O}_X$ is given as follows. Let U be open. Then the map $\mathcal{O}_X(U) \to \mathcal{O}_X(U)$ is given by $u \mapsto u^q$. This morphism is $\mathbb{F}_q$-linear and induces a $\mathbb{F}_q$-linear map on cohomology also denoted $F : \mathrm{H}^i(X, \mathcal{O}_X) \to \mathrm{H}^i(X, \mathcal{O}_X)$.

Our goal is to compute a formula relating $\mathbb{F}_q$-points on X and the trace of these Frobenius actions on cohomology. First we will generalize this setup to coherent sheaves on X with a Frobenius action which will lead us to the definition of F-modules.

Definition 2.1. Let $\mathcal{M}$ be a coherent sheaf on X. A Frobenius action on $\mathcal{M}$ is a morphism of sheaves $F_\mathcal{M} : \mathcal{M} \to F_*\mathcal{M}$, where F_* denotes the pushforward. That is, given an open U, $a \in \mathcal{O}_X(U)$ and $m \in \mathcal{M}(U)$, we have $F_\mathcal{M}(am) = a^q F_\mathcal{M}(m)$. This map is $\mathbb{F}_q$-linear which induces a linear morphism $F_\mathcal{M} : \mathrm{H}^i(X, \mathcal{M}) \to \mathrm{H}^i(X, \mathcal{M})$. The sheaf $\mathcal{M}$ along with the action $F_\mathcal{M}$ is called a coherent F-module denoted by $(\mathcal{M}, F_\mathcal{M})$. We denote the collection of coherent F-modules on X by $Coh_F(X)$.

To show that $Coh_F(X)$ is a category, we need to define morphisms between the objects.

Definition 2.2. Let $(\mathcal{M}, F_\mathcal{M})$ and $(\mathcal{M}', F'_\mathcal{M})$ be coherent F-modules on X. A morphism $(\mathcal{M}, F_\mathcal{M}) \to (\mathcal{M}', F'_\mathcal{M})$ is a morphism $\phi : \mathcal{M} \to \mathcal{M}'$ on the underlying sheaves that is compatible with the Frobenius actions. That is the diagram

$$\begin{array}{ccc} \mathcal{M} & \xrightarrow{\phi} & \mathcal{M}' \\ {\scriptstyle F_\mathcal{M}}\downarrow & & \downarrow{\scriptstyle F_{\mathcal{M}'}} \\ F_*\mathcal{M} & \xrightarrow{\phi} & F_*\mathcal{M}' \end{array}$$

commutes.

This makes $Coh_F(X)$ into a category. Notice that $Coh_F(X)$ is actually an abelian category. This is since kernels and cokernels may be defined as in the category of coherent sheaves on X. Then we have a Frobenius action on kernels and cokernels induced by $F_\mathcal{M}$, giving them the structure of F-modules.

Let x be a closed point of X. Then, we have the residue field $\mathbb{F}_q(x)$ which is the quotient of the stalk $\mathcal{O}_{X,x}$ by its maximal ideal. By the Nullstellensatz, $\mathbb{F}_q(x)$ is a finite extension of $\mathbb{F}_q$.

Definition 2.3. We define the $\mathbb{F}_q$-points of X by

$$X(\mathbb{F}_q) := \mathrm{Hom}(\operatorname{Spec} \mathbb{F}_q, X).$$

Take a morphism $\operatorname{Spec} \mathbb{F}_q \to X$ in $X(\mathbb{F}_q)$. Since $\mathbb{F}_q$ is a field, we know $\operatorname{Spec} \mathbb{F}_q$ has a unique element which maps to some $x \in X$.

The morphism induces a local ring morphism on stalks $\mathcal{O}_{X,x} \to \mathcal{O}_{\operatorname{Spec} \mathbb{F}_q,(0)}$. Taking quotients by the unique maximal ideals gives an inclusion on residue fields $\mathbb{F}_q(x) \to \mathbb{F}_q$. But since $\mathbb{F}_q(x)$ is a finite extension of $\mathbb{F}_q$, it must be that $\mathbb{F}_q(x) \cong \mathbb{F}_q$.

Conversely, if x is a point with residue field $\mathbb{F}_q$, then we have a local homomorphism $\mathcal{O}_{X,x} \to \mathbb{F}_q$. This gives a morphism of schemes $\operatorname{Spec} \mathbb{F}_q \to \operatorname{Spec} \mathcal{O}_{X,x}$. Composing this with the cannonical morphism $\operatorname{Spec} \mathcal{O}_{X,x} \to X$ gives a morphism $\operatorname{Spec} \mathbb{F}_q \to X$, which is an element of $X(\mathbb{F}_q)$. Thus, the $\mathbb{F}_q$-points of X are exactly the points with residue field equal to $\mathbb{F}_q$.

Let $x \in X(\mathbb{F}_q)$, so we have $\mathbb{F}_q(x) \cong \mathbb{F}_q$. Then, the Frobenius action $F_{\mathcal{M}}$ induces an $\mathbb{F}_q$-linear endomorphism on the fiber $\mathcal{M}(x) := \mathcal{M}_x \otimes \mathbb{F}_q(x)$. We denote this map by $F_{\mathcal{M}}(x)$.

2.2. **Grothendieck Groups.** In this section, we will introduce the Grothendieck group of coherent F-modules along with some important constructions.

Definition 2.4. We define the Grothendieck group of coherent F-modules on X, denoted $K_\bullet^F(X)$, to be the free abelian group generated by isomorphism classes of objects in $Coh_F(X)$ subject to the following relations.
First, addition is defined by short exact sequences. That is, if

$$0 \longrightarrow (\mathcal{M}', F') \longrightarrow (\mathcal{M}, F) \longrightarrow (\mathcal{M}'', F'') \longrightarrow 0$$

is exact, then we have

$$(\mathcal{M}, F) = (\mathcal{M}', F') + (\mathcal{M}'', F'').$$

Moreover, if F_1 and F_2 are Frobenius actions on $\mathcal{M}$, then we have

$$(\mathcal{M}, F_1 + F_2) = (\mathcal{M}, F_1) + (\mathcal{M}, F_2).$$

We denote the equivalence class of $(\mathcal{M}, F)$ in $K_\bullet^F(X)$ by $[\mathcal{M}, F]$. To simplify notation, if the Frobenius is clear, we may leave it out of the notation.

An important construction is the pushforward of Grothendieck groups. Given a proper morphism of schemes $f : X \to Y$, the higher direct image sheaves induce a morphism $K_\bullet^F(X) \to K_\bullet^F(Y)$. Recall that given a sheaf $\mathcal{M}$ on X, the higher direct image of $\mathcal{M}$, $R^i f_*(\mathcal{M})$, is the sheafification of the presheaf $U \mapsto \mathrm{H}^i(f^{-1}(U), \mathcal{M})$ on Y.

If $F_{\mathcal{M}}$ is a Frobenius action on $\mathcal{M}$, $F_{\mathcal{M}}$ induces a Frobenius endomorphism on $\mathrm{H}^i(f^{-1}(U), \mathcal{M})$, which glue to a Frobenius action on $R^i f_*(\mathcal{M})$. This makes $R^i f_*(\mathcal{M})$ into a coherent F-module on Y.

Define $f_* : K_\bullet^F(X) \to K_\bullet^F(Y)$ by

$$f_*([\mathcal{M}, F_{\mathcal{M}}]) = \sum_{i \geq 0} (-1)^i [R^i f_*(\mathcal{M})].$$

We need to show that f_* is well-defined. Let

$$0 \longrightarrow (\mathcal{M}', F') \longrightarrow (\mathcal{M}, F) \longrightarrow (\mathcal{M}'', F'') \longrightarrow 0$$

be exact. We need to show that $f_*([\mathcal{M}, F]) = f_*([\mathcal{M}', F']) + f_*([\mathcal{M}'', F''])$. Since $R^i f_*$ is a δ-functor, we have a long exact sequence

$$\cdots \longrightarrow R^i f_*(\mathcal{M}') \longrightarrow R^i f_*(\mathcal{M}) \longrightarrow R^i f_*(\mathcal{M}'') \longrightarrow R^{i+1} f_*(\mathcal{M}') \longrightarrow \cdots$$

Applying the relations to this exact sequence gives the identity.

Let F_1, F_2 be Frobenius actions on $\mathcal{M}$ and $\overline{F_i}$ be the Frobenius induced on a higher direct image. Note that $\overline{F_1 + F_2} = \overline{F_1} + \overline{F_2}$, so the second relation in Definition 2.4 is also satisfied. Thus, f_* is well-defined.

Lemma 2.5. *Let $f : X \to Y$ be a closed immersion and $g : Y \to Z$ be a proper morphism of schemes. Then $(g \circ f)_* = g_* \circ f_*$.*

Proof. We want to show that $(g \circ f)_* = g_* \circ f_*$. Expanding this out, we want to show

$$\sum_i (-1)^i [R^i (g \circ f)_* (\mathcal{M})] = \sum_i (-1)^i [R^i g_* (\sum_j (-1)^j [R^j f_* (\mathcal{M})])]$$

$$= \sum_{i,j} (-1)^{i+j} [R^i g_* (R^j f_* (\mathcal{M}))].$$

Since f is a closed immersion, we know that $R^j f_*(\mathcal{M}) = 0$ for $j \geq 1$ and also $R^i g_* \circ R^i f_* = R^i (g \circ f)_*$. Plugging this into the right side shows that it is indeed equal to the left. □

In the other direction, we have pullbacks. We first state a lemma.

Lemma 2.6. *If the F-module $(\mathcal{M}, F_\mathcal{M})$ has a nilpotent Frobenius $F_\mathcal{M}$, then we have $[\mathcal{M}, F_\mathcal{M}] = 0$.*

Proof. Since $F_\mathcal{M}$ is nilpotent, there exists some m such that $F_\mathcal{M}^m = 0$. We will prove this using induction on m. For the base case, $m = 1$ so $F_\mathcal{M} = 0$. In the Grothendieck group, we have the relation

$$[\mathcal{M}, 0] = [\mathcal{M}, 0] + [\mathcal{M}, 0]$$

since $0 + 0 = 0$. It follows that $[\mathcal{M}, 0] = 0$. For the inductive step, we have an exact sequence

$$0 \longrightarrow (\ker(F_\mathcal{M}), F'_\mathcal{M}) \longrightarrow (\mathcal{M}, F_\mathcal{M}) \longrightarrow (\mathcal{M}/\ker(F_\mathcal{M}), F''_\mathcal{M}) \longrightarrow 0 \ ,$$

where $F'_\mathcal{M}$ and $F''_\mathcal{M}$ are induced by the $F_\mathcal{M}$ on the respective sheaves. Notice that $F'_\mathcal{M} = 0$ and $F''_\mathcal{M}$ is nilpotent of degree at most $m - 1$. Then by the inductive assumption, we know that $[\ker(F_\mathcal{M}), F'_\mathcal{M}] = 0$ and $[\mathcal{M}/\ker(F_\mathcal{M}), F''_\mathcal{M}] = 0$. Finally by a relation in the Grothendieck group, we have that

$$[\mathcal{M}, F_\mathcal{M}] = 0 + 0 = 0.$$

□

Let $j : X \to Y$ be a closed immersion. We can define a pullback map $j^* : Coh_F(Y) \to K_\bullet^F(X)$ using pullbacks of sheaves by

$$j^*((M, F_\mathcal{M})) = [\mathcal{M} \otimes_{\mathcal{O}_Y} \mathcal{O}_X, \overline{F_\mathcal{M}}],$$

where $\overline{F_\mathcal{M}}$ is induced by $F_\mathcal{M}$ as follows.

Note that if $\mathcal{I}$ is the ideal sheaf of X in Y, the map j^* can be written as

$$j^*((M, F_\mathcal{M})) = [\mathcal{M}/\mathcal{I}\mathcal{M}, \overline{F_\mathcal{M}}].$$

Notice that $F_\mathcal{M}(\mathcal{I}\mathcal{M}) \subset \mathcal{I}^q \mathcal{M}$, so $F_\mathcal{M}$ is a well-defined Frobenius map on $\mathcal{M}/\mathcal{I}\mathcal{M}$. We denote $F_\mathcal{M}$ on $\mathcal{M}/\mathcal{I}\mathcal{M}$ by $\overline{F_\mathcal{M}}$. We claim that j^* is well-defined on the Grothendieck group $K_\bullet^F(Y)$ and that it is the inverse to the map j_*.

Lemma 2.7. *The map $j^* : K_\bullet^F(Y) \to K_\bullet^F(X)$ given by*

$$j^*([M, F_\mathcal{M}]) = [\mathcal{M} \otimes_{\mathcal{O}_Y} \mathcal{O}_X, \overline{F_\mathcal{M}}]$$

is well defined. Moreover, $j^* \circ j_*$ is the identity.

Proof. We need to check that j^* satisfies the relations in the definition of $K_\bullet^F(Y)$.

Let

$$0 \longrightarrow (\mathcal{M}', F'_{\mathcal{M}}) \longrightarrow (\mathcal{M}, F_{\mathcal{M}}) \longrightarrow (\mathcal{M}'', F''_{\mathcal{M}}) \longrightarrow 0$$

be exact. For the first relation, we need to show

$$j^*([\mathcal{M}]) = j^*([\mathcal{M}'] + [\mathcal{M}'']),$$

so we need to show

$$[\mathcal{M}/\mathcal{I}\mathcal{M}] = [\mathcal{M}'/\mathcal{I}\mathcal{M}'] + [\mathcal{M}''/\mathcal{I}\mathcal{M}''].$$

Note that the given exact sequence induces an exact sequence

$$0 \longrightarrow \mathcal{M}' \cap \mathcal{I}\mathcal{M} \longrightarrow \mathcal{I}\mathcal{M} \longrightarrow \mathcal{I}\mathcal{M}'' \longrightarrow 0$$

which gives us the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathcal{M}' \cap \mathcal{I}\mathcal{M} & \longrightarrow & \mathcal{I}\mathcal{M} & \longrightarrow & \mathcal{I}\mathcal{M}'' & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \mathcal{M}' & \longrightarrow & \mathcal{M} & \longrightarrow & \mathcal{M}'' & \longrightarrow & 0. \end{array}$$

The second half of the exact sequence given by the snake lemma gives an exact sequence

$$0 \longrightarrow \mathcal{M}'/\mathcal{M}' \cap \mathcal{I}\mathcal{M} \longrightarrow \mathcal{M}/\mathcal{I}\mathcal{M} \longrightarrow \mathcal{M}''/\mathcal{I}\mathcal{M}'' \longrightarrow 0.$$

Thus,

$$[\mathcal{M}/\mathcal{I}\mathcal{M}] = [\mathcal{M}'/\mathcal{M}' \cap \mathcal{I}\mathcal{M}] + [\mathcal{M}''/\mathcal{I}\mathcal{M}'']. \tag{2.8}$$

Notice that the surjection $\mathcal{M}'/\mathcal{I}\mathcal{M}' \to \mathcal{M}'/\mathcal{M}' \cap \mathcal{I}\mathcal{M}$ has kernel $\mathcal{M}' \cap \mathcal{I}\mathcal{M}/\mathcal{I}\mathcal{M}'$. This gives an exact sequence

$$0 \longrightarrow \mathcal{M}' \cap \mathcal{I}\mathcal{M}/\mathcal{I}\mathcal{M}' \longrightarrow \mathcal{M}'/\mathcal{I}\mathcal{M}' \longrightarrow \mathcal{M}'/\mathcal{M}' \cap \mathcal{I}\mathcal{M} \longrightarrow 0.$$

We then have the equality

$$[\mathcal{M}'/\mathcal{M}' \cap \mathcal{I}\mathcal{M}] = [\mathcal{M}'/\mathcal{I}\mathcal{M}'] - [\mathcal{M}' \cap \mathcal{I}\mathcal{M}/\mathcal{I}\mathcal{M}'].$$

Plugging this into (2.8) gives

$$[\mathcal{M}/\mathcal{I}\mathcal{M}] = [\mathcal{M}'/\mathcal{I}\mathcal{M}'] - [\mathcal{M}' \cap \mathcal{I}\mathcal{M}/\mathcal{I}\mathcal{M}'] + [\mathcal{M}''/\mathcal{I}\mathcal{M}''].$$

Thus, it is enough to show that $[\mathcal{M}' \cap \mathcal{I}\mathcal{M}/\mathcal{I}\mathcal{M}'] = 0$. By Lemma 2.6 we can do this by showing that the Frobenius is nilpotent. By Artin-Rees (see [Vak17] 12.9.4), there exists some k such that for all $j \geq k$

$$\mathcal{I}^j\mathcal{M} \cap \mathcal{M}' = \mathcal{I}^{j-k}((\mathcal{I}^k\mathcal{M}) \cap \mathcal{M}').$$

Then for large enough M,

$$\mathcal{I}^M\mathcal{M} \cap \mathcal{M}' \subset \mathcal{I}\mathcal{M}'.$$

Choose m such that $q^m > M$. Then,

$$F^m_{\mathcal{M}}(\mathcal{I}\mathcal{M} \cap \mathcal{M}') \subset \mathcal{I}^{q^m}\mathcal{M} \cap \mathcal{M}' \subset \mathcal{I}\mathcal{M}'.$$

Thus, $F_{\mathcal{M}}$ is nilpotent on $\mathcal{M}' \cap \mathcal{I}\mathcal{M}/\mathcal{I}\mathcal{M}'$. For the second relation we need to check that if F_1, F_2 are two Frobenius actions on $\mathcal{M}$, then $j^*([\mathcal{M}, F_1 + F_2]) = j^*([\mathcal{M}, F_1] + [\mathcal{M}, F_2])$. This amounts to showing that $\overline{F_1 + F_2} = \overline{F_1} + \overline{F_2}$. But this is clear by definition. It remains to show that $j^* \circ j_*$ is the identity. This follows from direct computation. □

This construction allows us to state a lemma that will be useful later.

Lemma 2.9. *Let X be the disjoint union of subschemes $X_1, ..., X_r$. Then, there is an isomorphism*

$$\bigoplus_{i=1}^{r} K_\bullet^F(X_i) \to K_\bullet^F(X).$$

Proof. We have inclusions $i_k : X_k \to X$. The sum of the pushforwards gives the map in the forward direction. The inverse is given by the pullbacks to the X_k's. □

2.3. **Computation of Grothendieck Groups.** We end the discussion on Grothendieck groups by computing the Grothendieck group of $\mathrm{Spec}(\mathbb{F}_q)$ and projective space. Both of these computations will be useful in the proof of Fulton's trace formula. We start by computing $K_\bullet^F(\operatorname{Spec}\mathbb{F}_q)$. This is where the trace of Frobenius enters the picture.

Theorem 2.10. *Trace defines an isomorphism $K_\bullet^F(\operatorname{Spec}\mathbb{F}_q) \cong \mathbb{F}_q$. That is, the map*

$$\varphi : [\mathcal{M}, F_\mathcal{M}] \mapsto \operatorname{tr}(F_\mathcal{M}(x))$$

is an isomorphism where x is the unique point corresponding to zero ideal.

Proof. Notice since $\operatorname{Spec}\mathbb{F}_q$ has a unique point, we can view a coherent module as a finite-dimensional $\mathbb{F}_q$-vector space, V, by looking at its global section. The Frobenius is then a endomorphism ϕ of this vector space. Thus, we can view elements of $Coh_F(\operatorname{Spec}\mathbb{F}_q)$ as such pairs (V, ϕ).

We have a map $\varphi : Coh_F(\operatorname{Spec}\mathbb{F}_q) \to \mathbb{F}_q$ given by $(V, \phi) \mapsto \operatorname{tr}(\phi)$. We need to show that this is a map on $K_\bullet^F(\operatorname{Spec}\mathbb{F}_q)$.

Let

$$0 \longrightarrow (V', \phi') \longrightarrow (V, \phi) \longrightarrow (V'', \phi'') \longrightarrow 0$$

be exact. Then $\operatorname{tr}(\phi) = \operatorname{tr}(\phi') + \operatorname{tr}(\phi'')$. Moreover, $\operatorname{tr}(\phi' + \phi'') = \operatorname{tr}(\phi') + \operatorname{tr}(\phi'')$. Thus, trace respects the relations on the Grothendieck group, so this map is well-defined on $K_\bullet^F(\operatorname{Spec}\mathbb{F}_q)$.

We have a map $\psi : \mathbb{F}_q \to K_\bullet^F(\operatorname{Spec}\mathbb{F}_q)$ given by sending x to $(\mathbb{F}_q, \cdot x)$, where $\cdot x$ is the map given by multiplication by x. The trace of this map is clearly x, so $\varphi \circ \psi = \mathrm{id}$.

We claim that ψ is surjective. This is enough to show that ψ is the inverse to the trace map. We will do this by induction. Let $[V, \phi] \in K_\bullet^F(\operatorname{Spec}\mathbb{F}_q)$. If V is one-dimensional, then $V = \mathbb{F}_q$ and ϕ is multiplication by some element of $\mathbb{F}_q$ so it clearly belongs to the image of ψ. Now suppose that V has dimension greater than one. We can write ϕ as a sum of morphisms with nontrivial invariant proper subspaces. Then without loss of generality, we suppose that ϕ has a nontrivial invariant proper subspace W. There is an exact sequence

$$0 \longrightarrow (W, \phi) \longrightarrow (V, \phi) \longrightarrow (V/W, \phi) \longrightarrow 0.$$

Then we can write $[V, \phi]$ as the sum $[W, \phi] + [V/W, \phi]$. Both W and V/W have dimension strictly less than V. Then by induction, the claim follows. Since ψ is surjective, we deduce that ψ is the inverse to the trace map, which completes the proof. □

Theorem 2.10 gives the structure of the Grothendieck group of $\mathrm{Spec}(\mathbb{F}_q)$. We can also compute the Grothendieck group of projective space, which will be useful later. We start with a lemma.

Lemma 2.11. *Let $(\mathcal{M}, F_{\mathcal{M}})$ be a F-module where $\mathcal{M} = \mathcal{M}_1 \oplus \cdots \oplus \mathcal{M}_r$. Denote by F_{ij} the composition $\mathcal{M}_i \longrightarrow \mathcal{M} \xrightarrow{F_{\mathcal{M}}} \mathcal{M} \longrightarrow \mathcal{M}_j$. Then,*

$$[\mathcal{M}, F] = \sum_{i=0}^{r} [\mathcal{M}_i, F_{ii}].$$

Proof. Denote by $\overline{F_{ij}}$ by the map $\mathcal{M} \to \mathcal{M}$ induced by F_{ij}, i.e. it is the composition $\mathcal{M} \longrightarrow \mathcal{M}_i \xrightarrow{F_{ij}} \mathcal{M}_j \longrightarrow \mathcal{M}$. We have that $F_{\mathcal{M}} = \sum_{ij} \overline{F_{ij}}$. The second relation in the Grothendieck group gives that

$$[\mathcal{M}, F_{\mathcal{M}}] = \sum_{ij} [\mathcal{M}, \overline{F_{ij}}].$$

Moreover, for $i \neq j$, $\overline{F_{ij}}^2 = 0$, so by Lemma 2.6, $[\mathcal{M}, \overline{F_{ij}}] = 0$. Thus,

$$[\mathcal{M}, F_{\mathcal{M}}] = \sum_{i=0}^{r} [\mathcal{M}, \overline{F_{ii}}] = \sum_{i=0}^{r} [\mathcal{M}_i, F_{ii}].$$

□

Now we turn to computing the Grothendieck group of projective space. Let S be the graded ring $\mathbb{F}_q[x_0, ..., x_n]$ and $X = \mathbb{P}^n_{\mathbb{F}_q} := \mathrm{Proj}\ S$. The structure sheaf will be denoted by $\mathcal{O}$.

We briefly describe the correspondence between coherent sheaves on X and finitely generated graded modules over S along with their corresponding Frobenius actions. More detail may be found in [Har77] 2.5.

First suppose that we have a F-module $(\mathcal{M}, F_{\mathcal{M}})$. We define M, the module associated to $\mathcal{M}$ as follows. Let $M = \Gamma_*(\mathcal{M}) := \bigoplus_{i \in \mathbb{Z}} \Gamma(X, \mathcal{M}(i))$. Given $s \in S_j$, we can view $s \in \Gamma(X, \mathcal{O}(j))$. Then if $t \in \Gamma(X, \mathcal{M}(i))$, $s \otimes t \in \Gamma(X, \mathcal{M}(i+j))$. Thus, M is a graded S-module with scalar multiplication given by tensor products.

The module M has an induced Frobenius from $F_{\mathcal{M}} : \mathcal{M} \to F_*(\mathcal{M})$ constructed as follows. Tensoring $F_{\mathcal{M}}$ with $\mathcal{O}(i)$ gives a map $\mathcal{M}(i) \to F_*(\mathcal{M}) \otimes \mathcal{O}(i)$. The projection formula gives a morphism

$$\mathcal{M}(i) \longrightarrow F_*(\mathcal{M}) \otimes \mathcal{O}(i) \longrightarrow F_*(\mathcal{M}(qi)) \ .$$

Looking at global sections defines a morphism $F_M : M \to M$ such that F_M is $\mathbb{F}_q$-linear, $F_M(st) = s^q F_M(t)$, where $s \in S$, $t \in M$. Moreover, $F_M(M_i) \subset M_{qi}$. A morphism F_M satisfying these properties is called a graded Frobenius action on M.

In the other direction, suppose that we have a finitely generated graded S-module M with a Frobenius action F_M. We take $\widetilde{M}$ to be the sheaf associated to the module M. We can define a Frobenius locally using the standard affine charts (U_i), where U_i is the chart where $x_i \neq 0$. Note that on U_i, we have $\Gamma(U_i, \widetilde{M}) = (M_{x_i})_0$. Then given $u \in M_N$, define

$$F_{\widetilde{M}}\left(\frac{u}{x_i^N}\right) = \frac{F_M(u)}{x_i^{qN}}.$$

This defines a Frobenius on $\widetilde{M}$. Hence we have operations taking coherent sheaves on X to finitely generated graded modules on S and vice-versa respecting the corresponding Frobenius actions. Moreover, notice that these operations are inverses. That is if $(\mathcal{M}, F_{\mathcal{M}})$ is an F-module, and M is the module associated with $\mathcal{M}$. Then $\mathcal{M} \cong \widetilde{M}$ as F-modules.

Proposition 2.12. *The Grothendieck group $K_\bullet^F(\mathbb{P}^n_{\mathbb{F}_q})$ is generated by the elements of the form $[\mathcal{O}(-i), x_0^{a_0} \cdots x_n^{a_n}]$, where $a_\ell \geq 0$ and $\sum_{\ell=0}^n a_\ell = i(q-1)$.*

Proof. Take $M = S(-i)$. Then notice that a Frobenius F_M is determined by $F_M(1)$. If $f \in S_i$, then

$$F_M(1) = F_M\left(\frac{1}{f}\ f\right) = \frac{f^q}{f}.$$

This is a homogeneous degree $i(q-1)$ polynomial. Conversely, every homogeneous polynomial of degree $i(q-1)$ determines a Frobenius. Then a Frobenius on M is determined by an element of $f \in S_{i(q-1)}$. The sheaf associated to $S(-i)$ is $\mathcal{O}(-i)$. By the second relation in $K_\bullet^F(\mathbb{P}^n_{\mathbb{F}_q})$, the element $[\mathcal{O}(-i), f]$ can be written as a sum of elements of elements $[\mathcal{O}(-i), x_0^{a_0} \cdots x_n^{a_n}]$, where $a_\ell \geq 0$ and $\sum_{\ell=0}^n a_\ell = i(q-1)$.

Now let M be an arbitrary graded S-module. By Hilbert's Syzygy Theorem, there exists (b_{ij}), with entries in $\mathbb{Z}$ such that $F_j := \bigoplus S(-b_{ij})$ forms a free resolution

$$0 \longrightarrow F_n \longrightarrow \cdots \longrightarrow F_1 \longrightarrow F_0 \longrightarrow M \longrightarrow 0\ .$$

This shows that

$$[\widetilde{M}] = \sum_{j=0}^{n} (-1)^j [\widetilde{F_j}].$$

Then since $[\widetilde{F_j}]$ can be written as a sum of elements of the form $[\mathcal{O}(-i), x_0^{a_0} \cdots x_n^{a_n}]$, using Lemma 2.11, $K_\bullet^F(\mathbb{P}^n_{\mathbb{F}_q})$ is generated by the elements $[\mathcal{O}(-i), x_0^{a_0} \cdots x_n^{a_n}]$. □

We can make an improvement on this list of generators.

Theorem 2.13. *The Grothendieck group $K_\bullet^F(\mathbb{P}^n_{\mathbb{F}_q})$ is generated by elements of the form $[\mathcal{O}(-i), x_0^{a_0}, ..., x_n^{a_n}]$, where $0 \leq a_\ell \leq q-1$, $\sum_{\ell=0}^n a_\ell = i(q-1)$ and there exists some ℓ such that $a_\ell < q-1$.*

Proof. First we need to eliminate generators with Frobenius containing some $a_\ell > q-1$. Suppose that $[\mathcal{O}(-i), f]$ is a generator where for some j the $x_j^{a_j}$ value in f has $a_j > q-1$. Then we can write $f = x_j^q g$. Let H be the hyperplane defined by $x_j = 0$. We have the exact sequence

$$S(-1) \xrightarrow{\cdot x_j} S \longrightarrow S/(x_j)\ .$$

Taking the sheaves associated to these modules gives the sequence

$$\mathcal{O}(-1) \xrightarrow{\cdot x_j} \mathcal{O} \longrightarrow \mathcal{O}_H\ .$$

Taking a twist by $-i+1$ gives the sequence

$$\mathcal{O}(-i) \xrightarrow{\cdot x_j} \mathcal{O}(-i+1) \longrightarrow \mathcal{O}_H(-i+1).$$

The Frobenius on $\mathcal{O}(-i)$ is $f = x_j^q g$. Then this will send $u \in \mathcal{O}(-i)$ to $u^q x_j x_j^q g = (ux_j)^q x_j g$. Thus the compatible Frobenius on $\mathcal{O}(-i+1)$ is given by $x_j g$. The Frobenius on $\mathcal{O}_H(-i+1)$ is 0 since x_j gets sent to 0 in $\mathcal{O}_H(-i+1)$. Then the relation in the Grothendieck group gives that

$$[\mathcal{O}(-i), f] = [\mathcal{O}(-i+1), x_j g].$$

Continuing this process, we can reduce until all the a_ℓ are less than or equal to $q-1$.

To complete the proof, we need to eliminate the generator

$$[\mathcal{O}(-n-1), (x_0 \cdots x_n)^{q-1}].$$

For this we consider a Koszul Complex of graded S-modules. Notice that $x_0, ..., x_n$ is a regular sequence in S. Let L_i be $S(-1)$ with the Frobenius action given by x_i^{q-1}. Denote $\mathscr{L}_i$ the sheaf associated with L_i. Then $E = L_0 \oplus \cdots \oplus L_n \cong S(-1)^{\oplus(n-1)}$ is a free S module of rank $n+1$. Given a L_i we have a map $L_i \to S$ given by multiplication by x_i. The sum of these maps, denoted ϕ, gives a map $E \to S$. This gives us the Koszul complex

$$0 \longrightarrow \bigwedge^{n+1} E \longrightarrow \cdots \longrightarrow \bigwedge^2 E \longrightarrow E \xrightarrow{\phi} S \longrightarrow 0 \ .$$

Taking the sheaves associated to these modules gives the complex

$$0 \longrightarrow \bigwedge^{n+1} \mathscr{E} \longrightarrow \cdots \longrightarrow \bigwedge^2 \mathscr{E} \longrightarrow \mathscr{E} \xrightarrow{\phi} \mathcal{O} \longrightarrow 0 \ ,$$

where $\mathscr{E} = \mathscr{L}_0 \oplus \cdots \oplus \mathscr{L}_n$ is the sheaf associated with E. Then,

$$\bigwedge^r \mathscr{E} = \bigoplus_{0 \le i_1 < \cdots < i_r \le n} (\mathscr{L}_{i_1} \otimes \cdots \otimes \mathscr{L}_{i_r}).$$

Note that

$$\mathscr{L}_{i_1} \otimes \cdots \otimes \mathscr{L}_{i_r} = \mathcal{O}(-r)$$

which has the Frobenius $x_{i_1}^{q-1} \cdots x_{i_r}^{q-1}$ which is compatible with the complex.

Then by relations, we can write $[\mathcal{O}(-n-1), (x_0 \cdots x_n)^{q-1}]$ as a sum of terms of the form $[\mathcal{O}(-r), x_{i_1}^{q-1} \cdots x_{i_r}^{q-1}]$ so we can eliminate it from the list of generators. □

2.4. **Localization Theorem.** An important piece of machinery needed in the proof of the trace formula is the localization theorem.

As in the previous setup, we have a scheme X over $\mathbb{F}_q$. We are interested in the $\mathbb{F}_q$-points of X, $X(\mathbb{F}_q)$.

Since we can view $X(\mathbb{F}_q)$ as a closed subscheme of X, we have a closed immersion $i : X(\mathbb{F}_q) \to X$. This induces a map $i_* : K_\bullet^F(X(\mathbb{F}_q)) \to K_\bullet^F(X)$ on Grothendieck groups. The localization theorem states that this is actually an isomorphism.

Theorem 2.14. *(Localization Theorem) The map $i_* : K_\bullet^F(X(\mathbb{F}_q)) \to K_\bullet^F(X)$ is an isomorphism.*

In this case of the localization theorem, we have a map i_* given by the inclusion $X(\mathbb{F}_q) \to X$. Lemma 2.7 shows that the map i^* is well-defined going in the other direction and that $i^* \circ i_*$ is the identity. To complete the proof of the localization theorem, it remains to show that $i_* \circ i^*$ is also the identity. In particular, it suffices to show that i_* is surjective.

We will first prove this in the case where X is projective space. To show this case, recall the structure of $K_\bullet^F(\mathbb{P}^n_{\mathbb{F}_q})$ given by Theorem 2.13. The general localization theorem will then follow from this special case.

Theorem 2.15. *The localization theorem, Theorem* 2.14*, holds for* $X = \mathbb{P}^n_{\mathbb{F}_q}$.

Proof. Let $i : \mathbb{P}^n(\mathbb{F}_q) \to \mathbb{P}^n_{\mathbb{F}_q}$ be the inclusion. Recall that we have shown that i_* is injective since $i^* \circ i_*$ is the identity. It remains to show that i_* is surjective. We can use a dimension argument. That is, we want to show that

$$\dim_{\mathbb{F}_q} K_\bullet^F(\mathbb{P}^n_{\mathbb{F}_q}) \leq \dim_{\mathbb{F}_q} K_\bullet^F(\mathbb{P}^n(\mathbb{F}_q)).$$

We have an upper bound for $\dim_{\mathbb{F}_q} K_\bullet^F(\mathbb{P}^n_{\mathbb{F}_q})$ given by counting the number of generators given by Theorem 2.13. We denote by α_n the number of generators of $K_\bullet^F(\mathbb{P}^n_{\mathbb{F}_q})$ given by Theorem 2.13.

We can view the generators as the set, A_n, defined as the set of n-tuples $(a_0, ..., a_n)$ satisfying $0 \leq a_i \leq q-1$, $q-1$ divides $\sum_{i=0}^n a_i$ and there exists some ℓ such that $a_\ell < q-1$. This is by viewing the n-tuples $(a_0, ..., a_n)$ as the powers in the generators described in Theorem 2.13.

We can compute α_n using a recurrence relation. Suppose that we have an $n-1$-tuple $(a_0, ..., a_{n-1})$. We consider two cases. If $(a_0, ..., a_{n-1}) \in A_{n-1}$, then $\sum_{i=0}^{n-1} a_i$ is divisible by $q-1$ and for some ℓ, $a_\ell < q-1$. Then we have two choices for a_n, 0 or $q-1$, which makes the tuple $(a_0, ..., a_n)$ belong to A_n. In the other case, if $(a_0, ..., a_{n-1}) \notin A_{n-1}$, there is only one option for a_n to make $(a_0, ..., a_n)$ belong to A_n. Thus, we have the relation

$$\alpha_n = 2\alpha_{n-1} + (q^n - \alpha_{n-1}) = q^n + \alpha_{n-1}.$$

Since $\alpha_0 = 1$, we have

$$\alpha_n = 1 + q + \cdots + q^n.$$

Then

$$\dim_{\mathbb{F}_q} K_\bullet^F(\mathbb{P}^n_{\mathbb{F}_q}) \leq 1 + q + \cdots + q^n.$$

Note that $\mathbb{P}^n(\mathbb{F}_q)$ has $1 + q + \cdots + q^n$ points. Then by Lemma 2.9, taking the subschemes as the points

$$\dim_{\mathbb{F}_q} K_\bullet^F(\mathbb{P}^n(\mathbb{F}_q)) = 1 + q + \cdots + q^n.$$

This completes the proof. □

The general case of the localization theorem follows from the projective case.

Proof. (Localization Theorem)
Denote the projective space $\mathbb{P}^n_{\mathbb{F}_q}$ by Y. Let j be a closed immersion $X \to Y$. Denote by j' the corresponding inclusion $X(\mathbb{F}_q) \to Y(\mathbb{F}_q)$. The map i is the inclusion $X(\mathbb{F}_q) \to X$ and i' the inclusion $i' : Y(\mathbb{F}_q) \to Y$. Then the diagram

$$\begin{array}{ccc} X(\mathbb{F}_q) & \xrightarrow{j'} & Y(\mathbb{F}_q) \\ \downarrow{\scriptstyle i} & & \downarrow{\scriptstyle i'} \\ X & \xrightarrow{j} & Y \end{array}$$

commutes. By the localization theorem for projective space, we have

$$i'_* \circ (i')^* = \mathrm{id}\,.$$

Also notice that

$$(i')^* \circ j_* = j'_* \circ i^*.$$

We know $i^* \circ i_* = \mathrm{id}$, we need to show $i_* \circ i^* = \mathrm{id}$. By commutativity of the diagram

$$j \circ i = i' \circ j'$$

so we have

$$j_* \circ i_* = i'_* \circ j'_*.$$

This gives

$$j_* \circ i_* \circ i^* = i'_* \circ j'_* \circ i^*.$$

Then,

$$j_* \circ i_* \circ i^* = i'_* \circ (i')^* \circ j_* = j_*,$$

since $j^* \circ j_* = \mathrm{id}$, j_* is injective. Thus,

$$i_* \circ i^* = \mathrm{id},$$

which completes the proof. □

2.5. **Proof of Fulton's Trace Formula.** Now we are ready to state and prove Fulton's Trace Formula.

Theorem 2.16. *(Fulton's Trace Formula) Let X be a scheme over $\mathbb{F}_q$ and $(\mathcal{M}, F_{\mathcal{M}})$ a coherent F-module on X. Then,*

$$\sum_{x \in X(\mathbb{F}_q)} \mathrm{tr}(F_{\mathcal{M}}(x)) = \sum_{i=0}^{\dim(X)} (-1)^i \,\mathrm{tr}(F_{\mathcal{M}} | H^i(X, \mathcal{M})).$$

Proof. Since X is a scheme over $\mathbb{F}_q$, we have a structure morphism $f : X \to \mathrm{Spec}\,\mathbb{F}_q$. Recall that this induces a map on Grothendieck groups f_*. The idea of the proof is to compute $f_*([\mathcal{M}, F_{\mathcal{M}}])$ in two ways.

Consider the diagram,

$$\begin{array}{ccc} K_\bullet^F(X) & \xrightarrow{i^*} & K_\bullet^F(X(\mathbb{F}_q)) \\ \downarrow{\scriptstyle f_*} & \swarrow{\scriptstyle f_* \circ i_*} & \\ K_\bullet^F(\mathrm{Spec}\,\mathbb{F}_q) & & \\ \downarrow{\scriptstyle trace} & & \\ \mathbb{F}_q & & \end{array}$$

This diagram commutes since the localization theorem shows that i_* and i^* are inverses. We first compute $f_*([\mathcal{M}, F_{\mathcal{M}}])$ directly. Then we will compute it by $f_* \circ i_* \circ i^*$ as in the other direction in the upper triangle. Then we apply the isomorphism induced by trace, as described in Theorem 2.10, to our computations which will give us the formula in $\mathbb{F}_q$.

We first compute $f_*([\mathcal{M}, F_{\mathcal{M}}])$ directly. By the definition of f_*, this is

$$f_*([\mathcal{M}, F_{\mathcal{M}}]) = \sum_{i=0}^{\dim(X)} (-1)^i [R^i f_*(\mathcal{M})]$$

$$= \sum_{i=0}^{\dim(X)} (-1)^i [\mathrm{H}^i(X, \mathcal{M}), F_{\mathcal{M}}].$$

The second equality follows from the fact that since $\operatorname{Spec}\mathbb{F}_q$ is a one-point space, the functors $R^i f_*$ coincide with sheaf cohomology functors H^i. The sum only goes up to $\dim(X)$ since by Grothendieck Vanishing, the higher cohomology groups all vanish.

Next we compute

$$f_*([\mathcal{M}, F_{\mathcal{M}}]) = f_* \circ i_* \circ i^* = (f \circ i)_* \circ i^*$$

the second equality coming from Lemma 2.5. By definition,

$$i^*([\mathcal{M}, F_{\mathcal{M}}]) = [\mathcal{M} \otimes \mathcal{O}_X, \overline{F_{\mathcal{M}}}].$$

By Lemma 2.9, $[\mathcal{M} \otimes \mathcal{O}_X, \overline{F_{\mathcal{M}}}]$ can be viewed as a sum in $K_\bullet^F(\operatorname{Spec}\mathbb{F}_q)$, through taking pullbacks of inclusions of points. Pullbacks of inclusions of points are the same as fibers at those points, so we have

$$[\mathcal{M} \otimes \mathcal{O}_X, \overline{F_{\mathcal{M}}}] = \sum_{x \in X(\mathbb{F}_q)} [\mathcal{M}(x), F_{\mathcal{M}}(x)].$$

Note that since $X(\mathbb{F}_q)$ has dimension 0, by Grothendieck Vanishing, the only cohomology group that remains is $R^0(f \circ i)_*$. Again since f is a map to a one-point space and i is an inclusion, we see

$$(f \circ i)_*([\mathcal{M} \otimes \mathcal{O}_X, \overline{F_{\mathcal{M}}}]) = \sum_{x \in X(\mathbb{F}_q)} [\mathcal{M}(x), F_{\mathcal{M}}(x)] \in K_\bullet^F(\operatorname{Spec}\mathbb{F}_q).$$

Thus, our computations show

$$\sum_{x \in X(\mathbb{F}_q)} [\mathcal{M}(x), F_{\mathcal{M}}(x)] = \sum_{i=0}^{\dim(X)} (-1)^i [\mathrm{H}^i(X, \mathcal{M}), F_{\mathcal{M}}].$$

Then by Theorem 2.10, trace gives an isomorphism $K_\bullet^F(\operatorname{Spec}\mathbb{F}_q) \to \mathbb{F}_q$. Applying this map to both sides, gives the desired formula. □

We will be most interested in the case of this formula regarding counting $\mathbb{F}_q$-points of X. This can be derived as follows.

Corollary 2.17. *Let X be a projective scheme over $\mathbb{F}_q$. Then,*

$$|X(\mathbb{F}_q)| = \sum_{i=0}^{\dim X} (-1)^i \operatorname{tr}(F | H^i(X, \mathcal{O}_X)) \pmod{p}.$$

Proof. This follows from Fulton's Trace Formula using the F-module $(\mathcal{O}_X, F)$. Notice that the fiber $\mathcal{O}_X(x) \cong \mathbb{F}_q$, so the Frobenius $F(x)$ is just the identity. Thus, the left side will count $X(\mathbb{F}_q)$. □

Remark 2.18. Fulton's trace formula actually holds for all proper schemes X over $\mathbb{F}_q$. We will not need this generalization for the remaining applications in this paper. See [Ful78] for the additional step needed to make this generalization.

2.6. **Classical Applications.** We end the discussion of Fulton's trace formula with a couple of applications to some classical problems. The first application is the Chevalley-Warning theorem.

Theorem 2.19. *(Chevalley-Warning) Let X be a projective variety over $\mathbb{F}_q$, a finite field of characteristic p, defined by homogenous polynomials $f_1, ..., f_r \in S := \mathbb{F}_q[x_0, ..., x_n]$. Let $d_1, ..., d_r$ be the degrees of $f_1, .., f_r$ and suppose that $d_1 + \cdots + d_r < n + 1$. Then,*

$$|X(\mathbb{F}_q)| = 1 \pmod{p}.$$

Proof. We will show this using induction on the number of polynomials. For the base case, suppose X is defined by one polynomial f of degree d. We have the exact sequence

$$0 \longrightarrow S(-d) \xrightarrow{f} S \longrightarrow S/(f) \longrightarrow 0$$

which induces an exact sequence of sheaves

$$0 \longrightarrow \mathcal{O}_{\mathbb{P}^n}(-d) \xrightarrow{f} \mathcal{O}_{\mathbb{P}^n} \longrightarrow i_*\mathcal{O}_X \longrightarrow 0$$

where i is the inclusion of X into projective space.

Cohomology then gives the long exact sequence

$$\cdots \longrightarrow \mathrm{H}^i(\mathbb{P}^n, \mathcal{O}_{\mathbb{P}^n}(-d)) \longrightarrow \mathrm{H}^i(\mathbb{P}^n, \mathcal{O}_{\mathbb{P}^n}) \longrightarrow \mathrm{H}^i(X, \mathcal{O}_X)$$

$$\longrightarrow \mathrm{H}^{i+1}(\mathbb{P}^n, \mathcal{O}_{\mathbb{P}^n}(-d)) \longrightarrow \cdots$$

From the computation of cohomology of projective space (see [Har77] 3(5.1)), since $d < n+1$, we have that for $i > 0$, $\mathrm{H}^i(\mathbb{P}^n, \mathcal{O}_{\mathbb{P}^n}(-d))$ is 0. From the same computation, we also have that $\mathrm{H}^i(\mathbb{P}^n, \mathcal{O}_{\mathbb{P}^n})$ is also 0 for $i > 0$. Thus, we deduce that for $i > 0$, $\mathrm{H}^i(X, \mathcal{O}_X)$ is 0.

We only need to compute the Frobenius action on $\mathrm{H}^0(X, \mathcal{O}_X)$. The beginning of the exact sequence is

$$0 \longrightarrow \mathbb{F}_q \longrightarrow \mathrm{H}^0(X, \mathcal{O}_X) \longrightarrow 0 \ .$$

Thus, $\mathrm{H}^0(X, \mathcal{O}_X) = \mathbb{F}_q$. But Frobenius acts by the identity on $\mathbb{F}_q$, so the trace is 1. Applying the trace formula gives the result.

Now suppose that we have two defining equations f_1, f_2. Define Z as the variety defined by f_1 and $S' := S/(f_1)$. Then we have an exact sequence

$$0 \longrightarrow S'(-d_2) \xrightarrow{f_2} S' \longrightarrow S'/(f_2) \longrightarrow 0 \ .$$

This gives an exact sequence of sheaves

$$0 \longrightarrow \mathcal{O}_Z(-d_2) \xrightarrow{f_2} \mathcal{O}_Z \longrightarrow i_*\mathcal{O}_X \longrightarrow 0 \ .$$

Consider the long exact sequence given by cohomology. By induction, the cohomology groups of $\mathcal{O}_Z$ are 0 except for $\mathrm{H}^0(Z, \mathcal{O}_Z)$ which is $\mathbb{F}_q$. The cohomology groups of $\mathcal{O}_Z(-d_2)$ are all 0. Then the only nonzero cohomology of $\mathcal{O}_X$ is $\mathrm{H}^0(X, \mathcal{O}_X) = \mathbb{F}_q$. Applying the trace formula again gives the result. We then continue inductively in this manner. □

A similar computation allows us to count the $\mathbb{F}_q$-points of hypersurfaces of degree $n+1$.

Theorem 2.20. *Let X be a projective variety over $\mathbb{F}_q$ defined by a polynomial f of degree $n+1$. Then,*

$$|X(\mathbb{F}_q)| = 1 + (-1)^{n-1}\alpha \pmod{p}$$

where α is the coefficient of $(x_0 \cdots x_n)^{q-1}$ in f^{q-1}.

Proof. Again consider the exact sequence

$$0 \longrightarrow \mathcal{O}_{\mathbb{P}^n}(-n-1) \xrightarrow{f} \mathcal{O}_{\mathbb{P}^n} \longrightarrow i_*\mathcal{O}_X \longrightarrow 0.$$

Take the long exact sequence given by cohomology. Similarly, $\mathrm{H}^0(X, \mathcal{O}_X) = \mathbb{F}_q$ and the middle cohomology $\mathrm{H}^k(X, \mathcal{O}_X)$ vanish for $0 < k < n-1$. The trace of Frobenius on $\mathbb{F}_q$ is 1. It remains to see how Frobenius acts on $\mathrm{H}^{n-1}(X, \mathcal{O}_X)$. At the end of the long exact sequence we have the sequence

$$0 \longrightarrow \mathrm{H}^{n-1}(X, \mathcal{O}_X) \xrightarrow{\delta} \mathrm{H}^n(\mathbb{P}^n, \mathcal{O}(-n-1)) \longrightarrow 0.$$

Then the boundary map δ is an isomorphism which we can use to understand the Frobenius, since $\mathrm{H}^n(\mathbb{P}^n, \mathcal{O}(-n-1))$ is well-understood.

The cohomology of projective space can be computed using Cech cohomology for the standard affine open cover $(D_+(x_i))$. The Cech complex for the sheaf $\mathcal{O}(-n-1)$ is

$$\prod (S_{x_{i_0}})_{(-n-1)} \longrightarrow \cdots \longrightarrow \prod (S_{x_0 \cdots \hat{x_i} \cdots x_n})_{(-n-1)} \xrightarrow{d} (S_{x_0 \cdots x_n})_{-n-1}.$$

Then $\mathrm{H}^n(\mathbb{P}^n, \mathcal{O}(-n-1))$ is the cokernel of d which is $(S_{x_0 \cdots x_n})_{-n-1}/\mathrm{im}(d)$. The ring $(S_{x_0 \cdots x_n})_{-n-1}$ has basis of monomials $x_0^{\ell_0} \cdots x_n^{\ell_n}$ where $\sum \ell_i = -n-1$. The image of d has basis of monomials where at least one of the powers is positive. Then $\mathrm{H}^n(\mathbb{P}^n, \mathcal{O}(-n-1))$ is generated by the monomials $x_0^{\ell_0} \cdots x_n^{\ell_n}$ where $\sum \ell_i = -n-1$ and $\ell_i < 0$ for all i, of which there is only one, $(x_0 \cdots x_n)^{-1}$.

Similarly, we find the cocycles of $\mathrm{H}^{n-1}(X, \mathcal{O}_X)$ to be

$$\prod ((S/(f))_{x_0 \cdots \hat{x_i} \cdots x_n})_0.$$

We can describe δ on the cocycles. Given $u \in \mathrm{H}^{n-1}(X, \mathcal{O}_X)$, we can choose a cocycle representative $(h_0, ..., h_n)$. Then $\delta(u)$ is the equivalence class of the element

$$w = \frac{\sum (-1)^i h_i}{f}.$$

Applying the Frobenius on u gives the representative $(h_0^q, ..., h_n^q)$ which gets mapped to $\frac{\sum (-1)^i h_i^q}{f} = f^{q-1} w^q$. Then the Frobenius acts on $\mathrm{H}^n(\mathbb{P}^n, \mathcal{O}(-n-1))$ through δ by $w \mapsto f^{q-1} w^q$. To figure out the trace, we need to see what happens to the basis element $(x_0 \cdots x_n)^{-1}$. The boundary map δ will take this to $f^{q-1}(x_0 \cdots x_n)^{-q}$. We need to take the equivalence class. Remember that all monomials with positive powers will get sent to 0 in this quotient. Then the only one which can remain is $\alpha(x_0 \cdots x_n)^{q-1}(x_0 \cdots x_n)^{-q} = \alpha(x_0 \cdots x_n)^{-1}$. Then the Frobenius acts by multiplication by α, so the trace is α. Plugging this into the trace formula gives the result. □

3. Elliptic Curves over $\mathbb{F}_p$

We now turn our focus to the specific case of elliptic curves. In particular, we will look at the Legendre family of elliptic curves. These are curves of the form $\mathbb{E}_\lambda : y^2 = x(x-1)(x-\lambda)$, parameterized by λ. We begin with an elementary computation of the number of $\mathbb{F}_p$-points on elliptic curves. Next, we will look at the Picard-Fuchs equation. This is a differential equation in λ which is derived from the cannonical differential and periods of elliptic curves. The Picard-Fuchs equation is a hypergeometric equation and we will be able to compute its solutions. It turns out that the solution to the Picard-Fuchs equation will coincide with the first computation of $\mathbb{F}_p$-points. We will turn to Fulton's trace formula developed in the previous section to investigate this strange phenomenon.

3.1. Rational Points Over $\mathbb{F}_p$.

In this section, we will compute the number of rational points of an elliptic curve over $\mathbb{F}_p$ mod p.

We will consider elliptic curves in Legendre form

$$E : y^2 = x(x-1)(x-\lambda)$$

where $\lambda \in \mathbb{F}_p$.

We will show the following.

Theorem 3.1. *The number of $\mathbb{F}_p$-points is given by*

$$|E(\mathbb{F}_p)| = 1 + (-1)(-1)^{\frac{p-1}{2}} \sum_{\ell=0}^{\frac{p-1}{2}} \binom{-\frac{1}{2}}{\ell}^2 \lambda^\ell \pmod{p}.$$

Given a, the number of solutions to $y^2 = a \pmod{p}$ is 2 if a is a square in $\mathbb{F}_p$, 0 if $a = 0 \pmod{p}$ and 1 otherwise. Then the number of solutions can be written as $(\frac{a}{p}) + 1$, where $(\frac{a}{p})$ is the Legendre symbol.

From this, we know that the number of $\mathbb{F}_p$ points can be written as,

$$1 + \sum_{x \in F_p} \left(\frac{x(x-1)(x-\lambda)}{p} \right) + 1, \tag{3.2}$$

where the additional 1 is given by the point at infinity.

The Legendre symbol can also be written as

$$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \pmod{p}.$$

Using this identity in (3.2) gives

$$|E(\mathbb{F}_p)| = 1 + \sum_{x \in \mathbb{F}_q} (x(x-1)(x-\lambda))^{\frac{p-1}{2}} + 1 \pmod{p}. \tag{3.3}$$

Let us focus on the term $\sum_{x \in \mathbb{F}_p} (x(x-1)(x-\lambda))^{\frac{p-1}{2}}$.

We first state a couple of lemmas.

Lemma 3.4. *(Fermat's Little Theorem) Given $a \in \mathbb{F}_p$, we have*

$$a^{p-1} = \begin{cases} 0 & p \mid k \\ 1 & p \nmid k \end{cases} \pmod{p}.$$

Lemma 3.5. *The sum $\sum_{x\in\mathbb{F}_p} x^k$ satisfies the identity*

$$\sum_{x\in\mathbb{F}_p} x^k = \begin{cases} -1 & p-1 \mid k \\ 0 & p-1 \nmid k \end{cases} \pmod p.$$

Proof. Notice that if $p-1 \mid k$, every term in the sum except for $x=0$ becomes a 1 by Lemma 3.4. Then it is easy to see that $\sum_{x\in\mathbb{F}_p} x^k = -1 \pmod p$ in this case. Now suppose that $p-1 \nmid k$. Let $y \neq 0$. We have

$$\sum_{x\in\mathbb{F}_p} (yx)^k = y^k \sum_{x\in\mathbb{F}_p} x^k \pmod p.$$

Note that since yx runs through all elements of $\mathbb{F}_p$, this is actually

$$\sum_{x\in\mathbb{F}_p} x^k = y^k \sum_{x\in\mathbb{F}_p} x^k \pmod p.$$

Then it must be that $\sum_{x\in\mathbb{F}_p} x^k = 0 \pmod p$ in this case. □

Lemma 3.5 allows us to make a very important reduction. When the sum $\sum_{x\in\mathbb{F}_q}(x(x-1)(x-\lambda))^{\frac{p-1}{2}}$ is expanded into a polynomial in x, all terms will go to 0 except for the terms of the form αx^{p-1}, which will become $-\alpha$. Thus, it is only necessary to find the coefficients of the terms with a x^{p-1}.

Notice that these coefficients exactly come from the coefficients of $x^{\frac{p-1}{2}}$ in the expansion of $((x-1)(x-\lambda))^{\frac{p-1}{2}}$.

Using the binomial theorem, we have

$$(x-1)^{\frac{p-1}{2}} = \sum_{k=0}^{\frac{p-1}{2}} \binom{\frac{p-1}{2}}{k} x^k (-1)^{\frac{p-1}{2}-k}$$

and

$$(x-\lambda)^{\frac{p-1}{2}} = \sum_{\ell=0}^{\frac{p-1}{2}} \binom{\frac{p-1}{2}}{\ell} x^\ell (-\lambda)^{\frac{p-1}{2}-\ell}.$$

Combining these equations, we see that $x^{\frac{p-1}{2}}$ terms appear when $k+\ell = \frac{p-1}{2}$, so the sum of the coefficients is

$$(-1)^{\frac{p-1}{2}} \sum_{k+\ell=\frac{p-1}{2}} \binom{\frac{p-1}{2}}{k}\binom{\frac{p-1}{2}}{\ell}\lambda^\ell.$$

By symmetry of the binomial coefficients, this is

$$(-1)^{\frac{p-1}{2}} \sum_{\ell=0}^{\frac{p-1}{2}} \binom{\frac{p-1}{2}}{\ell}^2 \lambda^\ell.$$

Notice that

$$\binom{\frac{p-1}{2}}{\ell} = \binom{-\frac{1}{2}}{\ell},$$

so the sum of coefficients is

$$(-1)^{\frac{p-1}{2}} \sum_{\ell=0}^{\frac{p-1}{2}} \binom{-\frac{1}{2}}{\ell}^2 \lambda^\ell.$$

Then we have the identity

$$\sum_{x\in\mathbb{F}_p}(x(x-1)(x-\lambda))^{\frac{p-1}{2}} = -(-1)^{\frac{p-1}{2}}\sum_{\ell=0}^{\frac{p-1}{2}}\binom{-\frac{1}{2}}{\ell}^2\lambda^\ell.$$

Plugging this into (3.3) completes the proof of Theorem 3.1.

Definition 3.6. The element

$$(-1)^{\frac{p-1}{2}}\sum_{\ell=0}^{\frac{p-1}{2}}\binom{-\frac{1}{2}}{\ell}^2\lambda^\ell$$

is known as the Hasse invariant of the elliptic curve $E : y^2 = x(x-1)(x-\lambda)$.

3.2. **Picard-Fuchs Equation.** In this section we will work again with the Legendre family of elliptic curves

$$E_\lambda : y^2 = x(x-1)(x-\lambda)$$

where $\lambda \in \mathbb{P}^1\setminus\{0,1,\infty\}$. This time we consider curves over the complex numbers $\mathbb{C}$. Topologically, the fibers in this family are all the same. They are all tori. However, as we move through the family, the complex structure of the tori will change. The complex structure will be given by periods on the elliptic curves which we will discuss shortly. We will derive the Picard-Fuchs equation which will be a differential equation satisfied by these periods.

On these elliptic curves E_λ, there is a canonical differential

$$\omega_\lambda = \frac{dx}{y}.$$

These differentials come from calculating the arc length of ellipses.

We wish to integrate this differential, but there is an issue concerning choice of path. Notice that E_λ is a double cover of $\mathbb{P}^1 \cong \hat{\mathbb{C}}$, ramified at $0, 1, \lambda, \infty$. To make this single valued, we must make some branch cuts. The following illustration demonstrates one such possible choice of cuts.

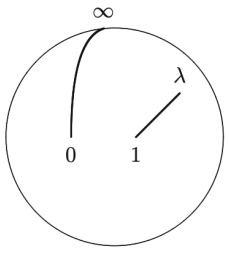

FIGURE 1. Branch cuts on E_λ. Figure from [Sil09].

The resulting Riemann surface is a torus. We choose paths α and β as depicted in the following figure.

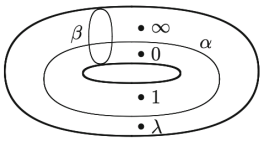

FIGURE 2. Paths α and β on E_λ. Figure from [Sil09].

Notice that the paths α and β generate the fundamental group of the torus. These paths define two values

$$\wp_1 = \int_\alpha \omega_\lambda$$
$$\wp_2 = \int_\beta \omega_\lambda.$$

These are called periods of E_λ. Let Λ be the lattice generated by the periods $\wp_1$ and $\wp_2$. By the prior discussion and the homology version of Cauchy's Theorem, we have a well defined map $E_\lambda \to \mathbb{C}/\Lambda$ given by

$$P \to \int_O^P \omega \pmod{\Lambda}.$$

This map is actually an isomorphism with inverse given by the Weierstrass $\wp$-function. In particular, the periods determine the complex structure of fibers in this family.

The periods $\wp_i$ can be considered as functions in the parameter λ. We wish to show that the $\wp_i$ satisfy a differential equation in λ and we want to compute the solutions.

Let $\Omega^1_{E_\lambda/\mathbb{C}}$ be the sheaf of relative 1-forms on E_λ over $\mathbb{C}$. Exterior derivatives give a complex

$$\Omega^\bullet_{E_\lambda/\mathbb{C}}: \ 0 \longrightarrow \mathcal{O}_{E_\lambda} \longrightarrow \Omega^1_{E_\lambda/\mathbb{C}} \longrightarrow 0 \longrightarrow \cdots$$

which is a resolution of the constant sheaf $\mathbb{C}$ on E_λ. We can compute de Rham cohomology using this resolution. Note that $\mathrm{H}^1(E_\lambda, \mathbb{C})$ has dimension 2.

We can differentiate the Canonical differential $\omega_\lambda = \frac{dx}{dy}$ with respect to λ. This gives the following 1-forms

$$\omega_\lambda = \frac{dx}{\sqrt{x(x-1)(x-\lambda)}}$$
$$\frac{\partial \omega_\lambda}{\partial \lambda} = \frac{1}{2}\frac{dx}{\sqrt{x(x-1)(x-\lambda)^3}}$$
$$\frac{\partial^2 \omega_\lambda}{\partial \lambda^2} = \frac{3}{4}\frac{dx}{\sqrt{x(x-1)(x-\lambda)^5}}$$

which belong in $\mathrm{H}^1_{dR}(E_\lambda)$. However, since this has dimension 2, there must be some linear dependency between these 1-forms.

Thus, we get a relation in de Rham group

$$A\frac{\partial^2\omega_\lambda}{\partial\lambda^2}+B\frac{\partial\omega_\lambda}{\partial\lambda}+C\omega_\lambda=\text{exact form.}$$

This gives the following differential equation on the periods

$$A\frac{\partial^2\wp_i}{\partial\lambda^2}+B\frac{\partial\wp_i}{\partial\lambda}+C\wp_i=0.$$

We can compute this relation explicitly.

By computation,

$$\begin{aligned}d\left(\frac{\sqrt{x(x-1)(x-\lambda)}}{(x-\lambda)^2}\right)&=(\frac{1}{2}x^{-1/2}(x-1)^{1/2}(x-\lambda)^{-3/2}\\&+\frac{1}{2}x^{1/2}(x-1)^{-1/2}(x-\lambda)^{-3/2}\\&-\frac{3}{2}x^{1/2}(x-1)^{1/2}(x-\lambda)^{-5/2})dx\\&=(x-1)\frac{\partial\omega_\lambda}{\partial\lambda}+x\frac{\partial\omega_\lambda}{\lambda}-2x(x-1)\frac{\partial^2\omega_\lambda}{\partial\lambda^2}.\end{aligned}$$

Make the substitutions

$$\begin{aligned}x-1&=(x-\lambda)+(\lambda-1)\\x&=(x-\lambda)+\lambda.\end{aligned}$$

Then we get

$$2(x-\lambda)\frac{\partial\omega_\lambda}{\partial\lambda}+(2\lambda-1)\frac{\partial\omega_\lambda}{\partial\lambda}-2(x-\lambda)^2\frac{\partial^2\omega_\lambda}{\partial\lambda^2}-2(2\lambda-1)(x-\lambda)\frac{\partial^2\omega_\lambda}{\partial\lambda^2}-2\lambda(\lambda-1)\frac{\partial^2\omega_\lambda}{\partial\lambda^2}.$$

We also know that

$$\begin{aligned}(x-\lambda)\frac{\partial\omega_\lambda}{\partial\lambda}&=\frac{1}{2}\omega_\lambda\\(x-\lambda)\frac{\partial^2\omega_\lambda}{\partial\lambda^2}&=\frac{3}{2}\frac{\partial\omega_\lambda}{\partial\lambda}.\end{aligned}$$

Making these substituions gives

$$-\frac{1}{2}\omega_\lambda-(4\lambda-2)\frac{\partial\omega_\lambda}{\partial\lambda}-2\lambda(\lambda-1)\frac{\partial^2\omega_\lambda}{\partial\lambda^2}.$$

Thus, we have the relation

$$-\frac{1}{2}d\left(\frac{\sqrt{x(x-1)(x-\lambda)}}{(x-\lambda)^2}\right)=\frac{1}{4}\omega_\lambda+(2\lambda-1)\frac{\partial\omega_\lambda}{\partial\lambda}+\lambda(\lambda-1)\frac{\partial^2\omega_\lambda}{\partial\lambda^2}.$$

Integrating on the path α or β, the generators of the fundamental group of the torus chosen earlier, gives the Picard-Fuchs equation

$$\lambda(\lambda-1)\frac{\partial^2\wp_i}{\partial\lambda^2}+(2\lambda-1)\frac{\partial\wp_i}{\partial\lambda}+\frac{1}{4}\wp_i=0.$$

This is a Gauss hypergeometric equation. More importantly, the structure of the solutions to this type of equation is well-known. These are computed using the

Frobenius method. We are interested in the solutions at the singular point $\lambda = 0$. The space of solutions has basis

$$y_1(\lambda) = \sigma_1(\lambda)$$
$$y_2(\lambda) = \lambda\sigma_2(\lambda) + (\log\lambda)\sigma_1(\lambda),$$

where σ_i are holomorphic functions which do not vanish at 0.

We can normalize so that

$$y_1(0) = 1.$$

We aim to find a power series expansion of y_1

$$y_1(\lambda) = \sum_{n=0}^{\infty} a_n\lambda^n.$$

The idea is to find a recurrence relation for the coefficients a_n.

Plugging y_1 into the differential equation gives

$$\sum_{n=0}^{\infty}\left(\lambda(\lambda-1)(n+2)(n+1)a_{n+2} + (2\lambda-1)(n+1)a_{n+1} + \frac{1}{4}a_n\right)\lambda^n = 0.$$

Reorganizing this sum by the powers of λ, we can write this sum as

$$\sum_{n=0}^{\infty}\left(\left(n+\frac{1}{2}\right)^2 a_n - (n+1)^2 a_{n+1}\right)\lambda^n = 0.$$

In particular,

$$\left(n+\frac{1}{2}\right)^2 a_n = (n+1)^2 a_{n+1}.$$

Since we normalized y_1 so that $y_1(0) = 1$, we also know that $a_0 = 1$. It follows that

$$a_n = \binom{-\frac{1}{2}}{n}^2,$$

so

$$y_1(\lambda) = \sum_{n=0}^{\infty}\binom{-\frac{1}{2}}{n}^2\lambda^n.$$

Surprisingly, we see that the Hasse invariant has made an appearance. It is a solution of the Picard-Fuchs equation, since it is a multiple of y_1. This raises a natural question of why this invariant determining the number of $\mathbb{F}_p$-points appears in this analytic situation. It is not a mere coincidence. In the next section, we will discuss the rather deep and beautiful relationship.

3.3. **Relationship Between the Picard-Fuchs Equation and $\mathbb{F}_p$-Points.** So far we have made two distinct computations. First, we computed the number of rational points on elliptic curves in $\mathbb{F}_p$ mod p. Then we considered the Legendre family of elliptic curves over $\mathbb{C}$. The periods corresponding to these elliptic curves satisfy the Picard-Fuchs differential equation. We then computed a holomorphic solution to this differential equation. Unexpectedly, the Hasse invariant which we showed in the first computation determines the number of $\mathbb{F}_p$-points is a solution to the Picard-Fuchs equation. The Picard-Fuchs equation which was derived using analytic information of the elliptic curve also contains arithmetic information about the curve. In this section, we will show the connection between the arithmetic side

and the analytic side.

This is where Fulton's trace formula appears, in particular this following version, which we showed in section 2.4:

Corollary 3.7. *Let X be a projective scheme over $\mathbb{F}_q$ a field of characteristic p. Then,*

$$|X(\mathbb{F}_q)| = \sum_{i=0}^{\dim X} (-1)^i \operatorname{tr}(F|H^i(X, \mathcal{O}_X)) \pmod{p}.$$

Fulton's trace formula tells us that $|E_\lambda(\mathbb{F}_p)|$ will depend solely on the trace of Frobenius on cohomology of the structure sheaf. Notably, by the computation in section 3.1, the trace of Frobenius is the Hasse invariant. In section 3.2, our computation showed that the Hasse invariant is a solution to the Picard-Fuchs equation. We want to know why. The question now boils down to why the trace of Frobenius on the cohomology of the structure sheaf is a solution of the Picard-Fuchs equation. The Picard-Fuchs equation was derived through some linear dependency in the cohomology on the cotangent sheaf. By Serre duality there is actually a connection between the cohomology of the structure sheaf and the cohomology of the cotangent sheaf. This connection will be the bridge between the number of $\mathbb{F}_p$-points of elliptic curves and the Picard-Fuchs equation.

We will summarize the key results of Serre duality that we will need. For full details, one may refer to chapter 3.7 of [Har77].

Let X be a projective scheme of dimension n over an algebraically closed field k.

Definition 3.8. Let ω_X° be a coherent sheaf and $t : \mathrm{H}^n(X, \omega_X^\circ) \to k$ a morphism. This pair is dualizing for X if for all coherent sheaves $\mathscr{F}$, composing the map t with the pairing

$$\operatorname{Hom}(\mathscr{F}, \omega_X^\circ) \times \mathrm{H}^n(X, \mathscr{F}) \to \mathrm{H}^n(X, \omega_X^\circ)$$

gives an isomorphism

$$\operatorname{Hom}(\mathscr{F}, \omega_X^\circ) \cong \mathrm{H}^n(X, \mathscr{F})'.$$

The morphism t is called a trace morphism.

Theorem 3.9. *If X is a projective scheme over a field k, then a dualizing sheaf for X exists.*

Proof. This proof is in [Har77] 3(7.5). □

The dualizing sheaf and the trace morphism seem quite mysterious. Fortunately, for curves, we can describe these objects explicitly.

The idea is analogous to Poincare duality in de Rham cohomology where we have a pairing of differential forms with a trace map given by integration. That is, given a smooth compact manifold M, we have the pairing

$$\mathrm{H}^k_{dR}(M) \times \mathrm{H}^{n-k}_{dR}(M) \to \mathbb{R}$$

$$[\omega] \times [\eta] \mapsto \int [\omega] \wedge [\eta].$$

On the algebraic side, it turns out that the dualizing sheaf is the cannonical sheaf, i.e. the top exterior power of the cotangent sheaf.

Theorem 3.10. *Let X be a projective nonsingular variety over an algebraically closed field. Then the dualizing sheaf is ω_X, where ω_X denotes the cannonical sheaf.*

Proof. This can be found in [Har77] 3(7.12). □

In particular, for a smooth projective curve C, the dualizing sheaf is the cotangent sheaf Ω^1_C. To visualize the analogy with integration, we need to develop residues on curves. The trace map will correspond to the sum of residues.

Theorem 3.11. *Let $p \in C$ be a closed point and K denote the function field of C. We have a unique k-linear residue map $\mathrm{res}_p : \Omega_K \to k$ satisfying the following properties.*

- $\mathrm{res}_p(\tau) = 0$ *for* $\tau \in \Omega_{C,p}$
- $\mathrm{res}_p(f^n df) = 0$ *for* $f \in K^*, n \neq 1$
- $\mathrm{res}_p(f^{-1}df) = v_p(f) \cdot 1$ *, where v_p is the valuation on the valuation ring $\mathcal{O}_{C,p}$.*

To compute residues, take a local parameter $t \in \mathcal{O}_{C,p}$. Then for $\tau \in \Omega_K$, we can write

$$\tau = \sum_{i<0} a_i t^i + g dt,$$

where $g \in \mathcal{O}_{C,p}$. Then the properties in Theorem 3.11 show that

$$\mathrm{res}_p(\tau) = a_{-1}.$$

We have a corresponding residue theorem.

Theorem 3.12. *If $\tau \in \Omega_K$, then $\sum_{p \in C} \mathrm{res}_P(\tau) = 0$.*

The idea now is that there is an exact sequence

$$\Omega_K \longrightarrow \bigoplus_{p \in C} \Omega_K/\Omega_{C,p} \longrightarrow \mathrm{H}^1(C, \Omega_C) \longrightarrow 0 \ .$$

Note that by the first property in Theorem 3.11, res_p is well-defined on $\Omega_K/\Omega_{C,p}$. There is a map

$$\bigoplus_{p \in C} \Omega_K/\Omega_{C,p} \to k$$

given by

$$\tau \mapsto \sum_p \mathrm{res}_p(\tau).$$

Since by the residue theorem, Ω_K is mapped to 0, this gives a well-defined map on the quotient $\mathrm{H}^1(C, \Omega_C)$

$$t : \mathrm{H}^1(C, \Omega_C) \to k,$$

which is the trace map.

Putting together the previous discussion, we have the following duality theorem.

Theorem 3.13. *(Serre Duality for Curves) Let C be a smooth projective curve. Then for any coherent sheaf $\mathscr{F}$ we have a pairing*

$$\mathrm{Hom}(\mathscr{F}, \Omega_C) \times \mathrm{H}^1(C, \mathscr{F}) \to \mathrm{H}^1(C, \Omega_C).$$

Composing this pairing with the map t given by the sum of residues gives an isomorphism

$$\mathrm{Hom}(\mathscr{F}, \Omega_C) \cong \mathrm{H}^1(C, \mathscr{F})',$$

where $\mathrm{H}^1(C,\mathscr{F})'$ *denotes the dual.*

Let us return to elliptic curves. Let E_λ be an elliptic curve in Legendre form. Using the identification $\mathrm{Hom}(\mathcal{O}_{E_\lambda},\Omega_{E_\lambda})\cong \mathrm{H}^0(E_\lambda,\Omega_{E_\lambda})$ and Serre duality with the structure sheaf $\mathcal{O}_{E_\lambda}$, we have that

$$\mathrm{H}^0(E_\lambda,\Omega_{E_\lambda})\cong \mathrm{H}^1(E_\lambda,\mathcal{O}_{E_\lambda})'.$$

In particular, $\mathrm{H}^1(E_\lambda,\mathcal{O}_{E_\lambda})$ has dimension 1.

By the trace formula, to compute $E_\lambda(\mathbb{F}_p)$, we need to compute the trace of Frobenius on $\mathrm{H}^0(E_\lambda,\mathcal{O}_{E_\lambda})$ and $\mathrm{H}^1(E_\lambda,\mathcal{O}_{E_\lambda})$. As computed before, the trace of Frobenius on $\mathrm{H}^0(E_\lambda,\mathcal{O}_{E_\lambda})$ is 1. We are after the trace of Frobenius on $\mathrm{H}^1(E_\lambda,\mathcal{O}_{E_\lambda})$ which is the Haase invariant. Serre duality allows us to understand this in terms of $\mathrm{H}^0(E_\lambda,\Omega_{E_\lambda})$ which will then relate to the Picard-Fuchs Equation.

We need some description of $\mathrm{H}^1(E_\lambda,\mathcal{O}_{E_\lambda})$. This can be computed using a Cech cover. Take the Cech cover given by

$$U=E_\lambda\setminus\{q\} \text{ and } V=E_\lambda\setminus\{q'\}$$

where $q,q'\in E_\lambda$. This gives the complex

$$\mathcal{O}_{E_\lambda}(U)\oplus\mathcal{O}_{E_\lambda}(V)\xrightarrow{\delta}\mathcal{O}_{E_\lambda}(U\cap V).$$

The sheaf $\mathcal{O}_{E_\lambda}(U)$ consists of functions with poles at q, and $\mathcal{O}_{E_\lambda}(V)$ consists of functions with poles at q'. The coboundary map δ is given by $(f,g)\mapsto f|_{U\cap V}-g|_{U\cap V}$. It follows that $\mathrm{H}^1(E_\lambda,\mathcal{O}_{E_\lambda})$ consists of functions on E_λ with poles at q and q' quotient the sum of functions with poles at q and functions with poles at q'. The Serre duality pairing is then given by

$$\begin{aligned}\mathrm{H}^0(E_\lambda,\Omega_{E_\lambda})\times\mathrm{H}^1(E_\lambda,\mathcal{O}_{E_\lambda})&\to\overline{\mathbb{F}_p}\\(\omega,h)&\mapsto \mathrm{res}_q(h\omega)+\mathrm{res}_{q'}(h\omega).\end{aligned}$$

Recall that $\mathrm{H}^1(E_\lambda,\mathcal{O}_{E_\lambda})$ is one-dimensional. By Riemann-Roch, the dimension of the space of functions with a pole at q of order at most one and a pole at q' of order at most one is 2. The dimension of the space of functions with only a pole at q' of order at most three is 3. Then we know that there exists a function, h, with poles only at q and q', where the pole at q is simple and the pole at q' has order at least two.

Let $q'\in E_\lambda$. For each λ we make a choice of $q_\lambda\in E_\lambda(\mathbb{F}_p)$ and let h_λ be the corresponding function with a simple pole at q_λ and a pole of order at least 2 at q'. What q_λ is and the reason we need to make a such a choice will become apparent shortly. The function h_λ is a generator of $\mathrm{H}^1(E_\lambda,\mathcal{O}_{E_\lambda})$, so we will only need to compute the Frobenius on h_λ. The Frobenius will send $h_\lambda(x)$ to the function $h_\lambda(x^p)$.

To determine the trace, we need to write $h_\lambda(x^p)$ in terms of the basis $h_\lambda(x)$. Let $\omega(\lambda)$ be the form corresponding to the dual basis element of $h_\lambda(x)$ in the identification $\mathrm{H}^0(E_\lambda,\Omega_{E_\lambda})\cong\mathrm{H}^1(E_\lambda,\mathcal{O}_{E_\lambda})'$. Then the trace will be given by $\mathrm{res}_{q_\lambda}h_\lambda(x^p)\omega(\lambda)+\mathrm{res}_{q'}h_\lambda(x^p)\omega(\lambda)$. However, since we chose h_λ to have a pole of order at least 2 at q', $\mathrm{res}_{q'}h_\lambda(x^p)\omega(\lambda)$ is 0 and all that's left to compute is $\mathrm{res}_{q_\lambda}h_\lambda(x^p)\omega(\lambda)$.

To make this computation, expand both $\omega(\lambda)$ and $h_\lambda(x^p)$ using a local parameter t at q_λ. Expanding $\omega(\lambda)$ we have

$$\omega(\lambda)=a_0(\lambda)dt+\sum_{i=1}^{\infty}a_i(\lambda)(t-q_\lambda)^i dt.$$

We want a_0 to not depend on λ. Since the Legendre family is locally trivial around some λ_0, we can make a choice of q_λ so that $a_0(\lambda)$ is constant. This is since $a_0(\lambda) = \omega(\lambda)(\frac{\partial}{\partial x})|_{q_\lambda}$. Define $\varphi_\lambda = \omega(\lambda)(\frac{\partial}{\partial x})$. Then a choice of q_λ making a_0 constant amounts to solving the differential equation $\frac{d}{d\lambda}\varphi_\lambda(q_\lambda) = 0$ with the initial condition given by $\varphi_{\lambda_0}(q_{\lambda_0})$. Then by scaling, we may assume that $a_0(\lambda) = 1$.

Since $h_\lambda(x)$ has a simple pole at q_λ, we can write it in the form

$$h_\lambda(t) = \frac{1}{(t-q_\lambda)} + \sum_{i=0}^{\infty} b_i(\lambda)(t-q_\lambda)^i.$$

Then,

$$h_\lambda(t^p) = \frac{1}{(t-q_\lambda)^p} + \sum_{i=0}^{\infty} b_i(\lambda)(t-q_\lambda)^{pi}.$$

This computation makes sense since we required that $q_\lambda \in E_\lambda(\mathbb{F}_p)$.

To find the residue of $h_\lambda(t^p)\omega(\lambda)$, we need the coefficient of $(t-q_\lambda)^{-1}$ in $h_\lambda(t^p)\omega(\lambda)$. We see that this is exactly $a_{p-1}(\lambda)$. Thus, the trace of Frobenius on $\mathrm{H}^1(E_\lambda, \mathcal{O}_{E_\lambda})$ is $a_{p-1}(\lambda)$.

Since $\omega(\lambda)$ can be written in terms of the basis given by the cannonical differential, independent of λ since we made $a_0(\lambda) = 1$, $1 + \sum_{i=0}^{\infty} a_i(\lambda)(t-q_\lambda)^i$ will also satisfy the Picard-Fuchs equation. That is we have a relation

$$\left(\lambda(\lambda-1)\frac{\partial^2}{\partial\lambda^2} + (2\lambda-1)\frac{\partial}{\partial\lambda} + \frac{1}{4}\right)(1 + \sum_{i=1}^{\infty} a_i(\lambda)(t-q_\lambda)^i) = \text{exact form}.$$

Write the exact form locally as a series

$$\frac{d}{dt}\left(\sum_{i=0}^{\infty} c_i(t-q_\lambda)^i\right).$$

Looking at the differential operator on the $(t-q_\lambda)^{p-1}$ terms gives that

$$\left(\lambda(\lambda-1)\frac{\partial^2}{\partial\lambda^2} + (2\lambda-1)\frac{\partial}{\partial\lambda} + \frac{1}{4}\right)(a_{p-1}(\lambda)(t-q_\lambda)^{p-1}) = \frac{d}{dt}c_p(t-q_\lambda)^p.$$

But, $\frac{d}{dt}c_p(t-q_\lambda)^p = pc_p(t-q_\lambda)^{p-1} = 0$, so $a_{p-1}(\lambda)$ is a solution to the Picard-Fuchs equation. It follows that the trace of Frobenius on $\mathrm{H}^1(E_\lambda, \mathcal{O}_{E_\lambda})$ is a solution to Picard-Fuchs. We now see why the solution to the Picard-Fuchs equation is related to the number of $\mathbb{F}_p$-points of elliptic curves.

In particular, on the arithmetic side, the number of $\mathbb{F}_p$ points mod p is determined by the Hasse invariant. Through Fulton's trace formula, the Hasse invariant is the trace of Frobenius on $\mathrm{H}^1(E_\lambda, \mathcal{O}_{E_\lambda})$. With the connection between $\mathrm{H}^1(E_\lambda, \mathcal{O}_{E_\lambda})$ and $\mathrm{H}^0(E_\lambda, \Omega_{E_\lambda})$ through Serre duality, we see why the trace of Frobenius will actually satisfy the Picard-Fuchs equation. Hence, Fulton's trace formula and Serre duality explains why the Picard-Fuchs equation encodes in its solutions arithmetic information on the $\mathbb{F}_p$-points of elliptic curves.

Acknowledgements

I would like to thank my mentor Nacho Darago for introducing me to this interesting topic and for his guidance along the way. I am very grateful to Professor Matthew Emerton for teaching me a lot about elliptic curves over the summer. I would also like to thank Ethan Schondorf and Alek Skenderi for many helpful conversations. Finally, I would like to thank Professor Peter May for holding the REU in such an unprecedented time.

References

[Bül16] Tim-Henrik Bülles, *Fulton's Trace Formula for Coherent Cohomology* `http://www.math.uni-bonn.de/people/huybrech/Buelles.pdf`, 2016

[Cle80] C. Herbert Clemens, *A Scrapbook of Complex Curve Theory*, The University Series in Mathematics, Plenum Press, New York, NY, 1980

[Ful78] William Fulton, *A Fixed Point Formula For Varieties Over Finite Fields* Math. Scand. 42, 189-196, 1978

[Har77] Robin Hartshorne, *Algebraic Geometry*, Graduate Texts in Mathematics, Springer, New York, NY, 1977

[Mus11] Mircea Mustata, *Zeta Functions in Algebraic Geometry*, `http://www.math.lsa.umich.edu/~mmustata/zeta_book.pdf`, 2011

[Sil09] Joseph H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, Springer, New York, NY, 2009

[Vak17] Ravi Vakil, *The Rising Sea: Foundations of Algebraic Geometry*, `http://math.stanford.edu/~vakil/216blog/FOAGnov1817public.pdf`, 2017