THE LEFSCHETZ FIXED POINT THEOREM AND SOLUTIONS TO POLYNOMIALS OVER FINITE FIELDS

ANG LI

Abstract. Abstract here.

Contents

1. Introduction

Suppose we have an equation with integer coefficients, e.g. $y^2 = x^3 + x$ and we want to understand its solutions over a finite field. If we consider the solutions over $\mathbb{C}$, the set of solutions is a complex manifold and can be studied using powerful tools of complex analysis and algebraic topology. However, since the set of solutions over a finite field is also finite, and any obvious topology makes the set into a finite discrete set, there is little hope of using topological tools over the finite field. The goal of this paper is to demonstrate the idea that counting points provides a good replacement for algebraic topology over finite fields by analyzing some examples. We begin by counting points in some specific examples:

Example 1.1. (The Projective Plane) $\mathbb{P}^n(\mathbb{F}_q)$ can be viewed as the collection of distinct lines in the vector space $\mathbb{F}_q^{n+1}$. Thus the cardinality of $\mathbb{P}^n(\mathbb{F}_q)$ can be calculated by counting number of distinct lines and we have

$$|\mathbb{P}^n(\mathbb{F}_q)| = \frac{(q^{n+1}-1)(q^{n+1}-q)...(q^{n+1}-q^{n-1})}{(q^n-1)(q^n-q)...(q^n-q^{n-1})}. \tag{1.2}$$

Observe that the number of points on projective plane over $\mathbb{F}_q$ is a polynomial in q.

In a similar way, we can calculate the cardinality of Grassmannian.

Example 1.3. (Grassmannians) $Gr(n,k)(\mathbb{F}_q)$ is the collection of distinct k-dimensional subspaces in the vector space $\mathbb{F}_q^n$. And the number of distinct k-dimensional subspaces is

$$|Gr(n,k)(\mathbb{F}_q)| = \frac{(q^n-1)(q^n-q)...(q^n-q^{k-1})}{(q^k-1)(q^k-q)...(q^k-q^{k-1})}. \tag{1.4}$$

Similar to projective plane, the number of points on Grassmannian over $\mathbb{F}_q$ is also a polynomial in q

Example 1.5. We compute the number of solutions of $y^2 = x^3 + x$ in finite fields $\mathbb{F}_q$ for a small prime powers:

q	Number of solutions
5	$4 = 5 + 2 \cdot (-0.447) \cdot 5^{1/2} + 1$
5^2	$32 = 5^2 + 2 \cdot (0.6) \cdot (5^2)^{1/2} + 1$
5^3	$148 = 5^3 + 2 \cdot (0.98) \cdot (5^3)^{1/2} + 1$
7	$8 = 7 + 2 \cdot (0) \cdot 7^{1/2} + 1$
7^2	$64 = 7^2 + 2 \cdot (1) \cdot (7^2)^{1/2} + 1$
7^3	$344 = 7^3 + 2 \cdot (0) \cdot (7^3)^{1/2} + 1$
11	$12 = 11 + 2 \cdot (0) \cdot 11^{1/2} + 1$
11^2	$144 = 11^2 + 2 \cdot (1) \cdot (11^2)^{1/2} + 1$
11^3	$1332 = 11^3 + 2 \cdot (0) \cdot (11^3)^{1/2} + 1$

Notice that the number of solutions in the finite field $\mathbb{F}_q$ is in the form $q + 2 \cdot d(q) \cdot q^{1/2} + 1$, where $d(q)$ is a constant depending on q with absolute value less than 1. This connection is interesting because the number of solutions on the finite field $\mathbb{F}_q$ look almost like a polynomial function of q.

In order to understand this connection, first we need to re-interpret the number of points on a variety as the number of fixed points of an algebraic map. Let X be the solutions of the equation in $\bar{\mathbb{F}}_q$. Then the number of solutions in $\mathbb{F}_q$ is just the number of fixed points under the Frobenius map on X, sending x to x^q. And to count the number of fixed point of the Frobenius map, we can apply the following Lefschetz fixed point theorem in the complex case:

Theorem 1.6. *(The Lefschetz fixed point theorem) Let X be a closed smooth manifold and let $f : X \to X$ be a smooth map with all fixed points nondegenerate. Then*

$$L(f) = \sum_i (-1)^i Tr(f_* : H_i(X;\mathbb{Q}) \to H_i(X;\mathbb{Q})). \tag{1.7}$$

Using Lefschetz theorem, we can calculate the number of fixed points of the Frobenius map by calculating traces of the induced homomorphisms on homology groups and the number of fixed points is just the number of points on the variety.

To prove the Lefschetz fixed point theorem, notice that the number of fixed point of a map is the number of points in the intersection of graph with the diagonal and we'll also need Kunneth formula and Poincare duality to express the interseciont using homology.we'll start with background knowledge on intersection theory and algebraic topology in section 2. Then we'll prove the Lefschetz fixed point theorem in section 3 and look at counting fixed point of Froenius map in section 4.

2. Background knowledge on manifold and algebraic topology

We begin with some background knowledge on intersection theory and algebraic topology.

The following will be assumed in this section: X, Y, Z are boundaryless manifolds, X is compact, Z is a closed submanifold of Y and X and Z have dimensions, i.e. dim $X+$ dim $Z =$ dim Y.

Definition 2.1. If $f : X \to Y$ is transversal to Z, then $f^{-1}(Z)$ is a finite number of points, each with orientation number 1 or -1 by the preimage orientation. Define the *intersection number* $I(f, Z)$ to be the sum of these orientation numbers. Given any point x, such that $f(x) = z \in Z$, we have

$$df_x T_x(X) \oplus T_z(Z) = T_z(Z) \tag{2.2}$$

by transversality condition. Then the orientation number at x is 1 if the orientation on $df_x T_x(X) \oplus T_z(Z)$ is the same as the prescribed orientation on $T_z(Y)$, and -1 otherwise.

Proposition 2.3. *If $X = \partial W$ and $f : X \to Y$ extends to W, then $I(f, Z) = 0$.*

Proof. Suppose f extends to F, which we may assume to be transversal to Z by the Extension Theorem. And thus $f^{-1}(Z) = \partial F^{-1}(Z)$. Since $F^{-1}(Z)$ is an one-manifold with boundary, $I(f, Z) = 0$. □

Proposition 2.4. *In particular, homotopic maps always have the same intersection number.*

Then we can define the intersection number for any function.

Definition 2.5. Given any $g : X \to Y$, pick f such that f is homotopic to g and f is transversal to Z. Define the intersection number $I(g, Z) = I(f, Z)$.

By the previous proposition, the intersection number is well defined.

Definition 2.6. When Y is connected and X has the same dimension as Y, we define the degree of an arbitrary smooth map $f : X \to Y$ to be the intersection number $I(f, \{y\})$.

Proposition 2.7. *Suppose that $f : X \to Y$ is a smooth map of compact oriented manifolds having the same dimension and that $X = \partial W$. If f can be extended to all of W, then deg$(f) = 0$.*

Proposition 2.8. *Let W be a smooth compact region in $\mathbb{C}$ whose boundary contains no zeros of the polynomial p. Then the total number of zeros of p inside W counting multiplicities is the degree of the map $p/|p| : \partial W \to S^1$.*

Proposition 2.9. *$f \pitchfork g$ if and only if $f \times g \pitchfork \Delta$, and then*

$$I(f, g) = (-1)^{dim Z} I(f \times g, \Delta). \tag{2.10}$$

Definition 2.11. For arbitrary maps $f : X \to Y$, $g : Z \to Y$, we define $I(f, g) = (-1)^{dim Z} I(f \times g, \Delta)$.

Proposition 2.12. *If f_0 and g_0 are respectively homotopic to f_1 and g_1, then $I(f_0, g_0) = I(f_1, g_1)$.*

Proposition 2.13. $I(f, g) = (-1)^{(dim X)(dim Z)} I(g, f)$.

Let X be a closed oriented smooth manifold of dimension n. Let A and B be oriented smooth submanifolds of X of dimensions $n - i$ and $n - j$ respectively and intersect transversally. Then $A \cap B$ is a submanifold of dimension $n - (i + j)$. When $i + j = n$, $A \cap B$ is a finite set of points.

By Poincore duality, there is a isomorphism $D : H^i(M, \mathbb{Z}) \to H_{n-i}(M)$ such that $D(\alpha) = [M] \frown \alpha$. Let $[A], [B], [A \cap B]$ be images of the fundamental classes of $A, B, A \cap B$ under the inclusion map into X. Then we have $[A] \in H_{n-i}(X)$,

$[B] \in H_{n-j}(X)$ and $[A \cap B] \in H_{n-(i+j)}(X)$. We denote their Poincare duals by $[A]^{\cdot}$, $[B]^{\cdot}$ and $[A \cap B]^{\cdot}$. Cup product in Poincare dual to intersection:

Theorem 2.14. $[A]^* \smile [B]^* = [A \cap B]^*$.

We can use Poincare duality to define a intersection pairing for homology groups.

Definition 2.15. Given X a closed oriented manifold of dimension n, we define the *intersection pairing*

$$\cdot : H_{n-i}(X) \otimes H_{n-j}(X) \to H_{n-i-j}(X) \tag{2.16}$$

by first applying Poincare duality, taking the cup product and then applying Poincare duality again:

$$\alpha \cdot \beta = [X] \frown (\alpha^* \smile \beta^*). \tag{2.17}$$

And by previous Theorem, we have

$$[A] \cdot [B] = [A \cap B]. \tag{2.18}$$

When A and B have complementary dimensions and X is connected, we have $[A] \cdot [B] \in H_0(X) = \mathbb{Z}$ is the signed number of intersection points.

Then we calculate the cohomology group of the complex points of the algebraic varieties from earlier examples: the projective plane, Grassmannian and solutions of the equation $y^2 = x^3 + x$. We first calculate the cohomology groups for the complex projective plane by cell decomposition.

Example 2.19. (The Complex Projective Plane) $\mathbb{CP}^n$ has the cell decomposition

$$\mathbb{CP}^n = [1 : x_1 : .. : x_n] \sqcup [0 : x_1 : ... : x_n] = [1 : x_1 : ... : x_n] \sqcup \mathbb{CP}^{n-1}, \tag{2.20}$$

where $[1 : x_1 : ... : x_n]$ is isomorphic to the $\mathbb{C}^n$. Inductively, we have

$$\mathbb{CP}^n = \mathbb{C}^n \sqcup \mathbb{C}^{n-1} \sqcup ... \sqcup \mathbb{C} \sqcup [0 : ... : 0 : 1]. \tag{2.21}$$

Since $\mathbb{C}$ is a dimension 2 manifold, $\mathbb{CP}^n$ has no odd dimensional cell. Thus, $H_i(\mathbb{CP}^n, \mathbb{Z}) = 0$ for i odd and $H_i(\mathbb{CP}^n, \mathbb{Z}) = \mathbb{Z}$ for $0 \leq i \leq 2n$ even. Using the universal coefficients theorem for cohomology, the same is true for cohomology group.

Also $H^*(\mathbb{CP}^n, \mathbb{Z}) = \cup_{i=0}^{2n} H_i(\mathbb{CP}^n, \mathbb{Z})$ has a graded ring structure under the cup product. Given a generator T of the group $H^2(\mathbb{CP}^n, \mathbb{Z})$, it's the fundamental class of a hyperplane and T is also a ring generator. Thus we have

$$H^*(\mathbb{CP}^n, \mathbb{Z}) = \mathbb{Z}[T]/(T^{n+1}). \tag{2.22}$$

Similarly, we can calculate the cohomology groups of the Grassmannian by a Schubert cell decomposition.

Example 2.23. (Grassmannian) Let $Gr(n, k)$ denote the Grassmannian that parametrizes k-dimensional linear subspaces of n-dimensional vector space $\mathbb{C}^n$. Fix the flag to be the standard flag of $\mathbb{C}^n$. Then the Gr^n_k has a decomposition as the disjoint union of Schubert cells:

$$Gr(n, k) = \sqcup_{\mathbf{j} \in [n]} \mathcal{C}_{\mathbf{j}}, \tag{2.24}$$

where for each index $\mathbf{j} = \{j_1, ..., j_k\}$, the Schubert cell $\mathcal{C}_{\mathbf{j}}$ has a unique representation as a $k \times n$ matrix in row echelon form, where (l, j_l) position contains 1 and zeros above, below and to the right in l-th row. Note that the Schubert cell $\mathcal{C}_{\mathbf{j}}$

has dimension $\sum_l (j_l - l)$. To calculate the cohomology of $Gr(n,k)$, we quote the following proposition from Hatcher.

Proposition 2.25. *The cells $\mathcal{C}_j$ are the cells of a CW structure on $Gr(n,k)$.*

Furthermore, the cell $\mathcal{C}_{\mathbf{j}} \cong \mathbb{C}^{\sum j_l - l}$. Hence, $Gr(n,k)$ has just even dimensional cells.

For instance, when $n = 4$ and $k = 2$, the Grassmannian $Gr(4,2)$ can be decomposed to 6 Schubert cells with $\mathbf{j} = \{1,2\}, \{1,3\}, \{1,4\}, \{2,3\}, \{2,4\}, \{3,4\}$. With respect to the standard flag, they are parametrized as follows:

$$(2.26)\quad \mathcal{C}_{\{1,2\}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}; \mathcal{C}_{\{1,3\}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & * & 1 & 0 \end{pmatrix}; \mathcal{C}_{\{1,4\}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & * & * & 1 \end{pmatrix};$$

$$(2.27)\quad \mathcal{C}_{\{2,3\}} = \begin{pmatrix} * & 1 & 0 & 0 \\ * & 0 & 1 & 0 \end{pmatrix}; \mathcal{C}_{\{2,4\}} = \begin{pmatrix} * & 1 & 0 & 0 \\ * & 0 & * & 4 \end{pmatrix}; \mathcal{C}_{\{3,4\}} = \begin{pmatrix} * & * & 1 & 0 \\ * & * & 0 & 1 \end{pmatrix}.$$

Thus cells of $Gr(4,2)$ have dimension $0,2,4,4,6,8$. Thus we have $H_i(Gr(4,2)) = \mathbb{Z}$ for $i = 0,2,6,8$ and $H_i(Gr(4,2)) = \mathbb{Z}^2$ for $i = 4$. By Poincare duality, the cohomology group is the same.

(Ring structure)

The cohomology groups of the elliptic curve $y^2 = x^3 + x$ in $\mathbb{C}$ can be calculated using some facts from complex analysis.

Example 2.28. Let $E(\mathbb{C})$ denote the elliptic curve $y^2 = x^3 + x$ for $x, y \in \mathbb{C}$. By the theory of elliptic curves from complex analysis, we have $E(\mathbb{C}) = \mathbb{C}/\Lambda$, where Λ is the lattice generated by 1 and i.

The quotient $\mathbb{C}/\Lambda$ can be identified as the torus $S^1 \times S^1$, with homology groups $H_0(S^1 \times S^1; \mathbb{Z}) = H_2(S^1 \times S^1; \mathbb{Z}) = \mathbb{Z}$ and $H_1(S^1 \times S^1; \mathbb{Z}) = \mathbb{Z}^2$. Using the universal coefficients theorem for cohomology, we know that the associated Betti numbers are $1, 2, 1, 0, ...$ for $E(\mathbb{C})$. Notice that the coefficient of $(q^1/2)^k$ is the corresponding k-th Betti number of $E(\mathbb{C})$.

3. Lefschetz fixed point theorem

We now use intersection theory to prove the Lefschetz fixed point theorem. We first define the global Lefschetz number and introduce some properties of the Lefschetz number.

Definition 3.1. The global Lefschetz number of f is the intersection number $I(\Delta, graph(f))$, denoted $L(f)$.

Then we have the following theorem directly from the definition of Lefschetz number.

Theorem 3.2. *(Smooth Lefschetz Fixed-Point Theorem) Let $f : X \to X$ be a smooth map on a compact orientable manifold. If $L(f) \neq 0$, then f has a fixed point.*

Proposition 3.3. *$L(f)$ is a homotopy invariant.*

Let $f : X \to X$ be a smooth map. A *fixed point* of f is a point $p \in X$ such that $f(p) = p$. Then we have:

Theorem 3.4. *(The Lefschetz fixed point theorem) Let X be a closed smooth manifold and let $f : X \to X$ be a smooth map with all fixed points nondegenerate. Then*

$$L(f) = \sum_i (-1)^i Tr(f_* : H_i(X;\mathbb{Q}) \to H_i(X;\mathbb{Q})). \tag{3.5}$$

It follows from the universal coefficient theorem that the above traces are integers.

Definition 3.6. Define the *diagonal* to be

$$\Delta = \{(x,x)|x \in X\}. \tag{3.7}$$

Also define the *graph* of f to be

$$\Gamma(f) = \{(x,f(x))|x \in x\}. \tag{3.8}$$

Since p is a fixed point is equivalent to $p \in \Delta \cap \Gamma(f)$, to prove the Lefschetz theorem, we will look at $\Delta \cap \Gamma(f) \subset X \times X$. We also have

Lemma 3.9. *f has nondegenerate fixed points if and only if $\Gamma(f)$ and Δ intersect transversally in $X \times X$. In that case, for each fixed point p, the local Lefschetz number at p agrees with the sign of intersection of $\Gamma(f)$ and Δ at (p,p).*

It follows that if f has only nondegerate fixed points, we have

$$L(f) = [\Gamma(f) \cap \Delta] = [\Gamma(f)] \cdot [\Delta]. \tag{3.10}$$

To prove the Lefschetz theorem, we just need to compute the intersection number $[\Gamma(f)] \cdot [\Delta]$.

Recall that for any topological spaces X and Y there is a homology cross product

$$\times : H_i(X) \otimes H_j(Y) \to H_{i+j}(X \times Y). \tag{3.11}$$

If X and Y are smooth manifolds and A and B are closed oriented submanifolds of X and Y, then we have

$$[A] \times [B] = [A \times B]. \tag{3.12}$$

Let $n = dim(X)$. For $\alpha \in H_*(X)$ of pure degree, we denote the degree by $|\alpha|$. We have the following lemmas

Lemma 3.13. *Let $\alpha, \beta, \gamma, \delta \in H_*(X)$ with $|\alpha| + |\beta| = |\gamma| + |\delta| = n$. Then*

$$(\alpha \times \beta) \cdot (\gamma \times \delta) = (-1)^{|\beta|}(\alpha \cdot \gamma)(\beta \cdot \delta), \tag{3.14}$$

if $|\beta| = |\gamma|$; and 0 otherwise.

Lemma 3.15. *If $\alpha, \beta \in H_*(X)$ with $|\alpha| + |\beta| = n$, then*

$$[\Gamma(f)] \cdot (\alpha \times \beta) = (-1)^{|\alpha|} f_*\alpha \cdot \beta. \tag{3.16}$$

Note that if $\alpha, \beta, \gamma, \delta$ can be represented by submanifolds, the above lemmas can be proved by Theorem 1.1. In general, these two lemmas follow from the basic properties of cup products and we skip the computation here.

Let $\{e_k\}$ be a basis for the vector space $H_*(X;\mathbb{Q})$ and let $\{e'_k\}$ be the dual basis of $H_*(X;\mathbb{Q})$, with respect to the intersection pairing $\cdot$, i.e., $e_i \cdot e'_j = \delta_{i,j}$. This dual basis exists and is unique since the intersection paring is a perfect paring.

By Kunneth theorem $H_*(X \times X;\mathbb{Q}) = H_*(X;\mathbb{Q}) \otimes H_*(X;\mathbb{Q})$, with the isomorphism given by homology cross product. Then $\{e_i \times e'_j\}$ is a basis for $H_*(X \times X;\mathbb{Q})$. Then we can write $[\Delta]$ in terms of these basis elements:

Lemma 3.17. $[\Delta] = \sum_k e_k \times e'_k$.

Proof. Since $\{e'_i \times e_j\}$ is also a basis, it is sufficient to check that both sides have the same intersection pairing with $e'_i \times e_j$ for any $|e'_i| + |e_j| = n$.

$$\begin{aligned} (\sum_k e_k \times e'_k) \cdot (e'_i \times e_j) &= \sum_{k:|e'_k|=|e'_i|} (-1)^{|e'_i|}(e_k \cdot e'_i)(e'_k \cdot e_j) \quad (3.18) \\ &= (-1)^{|e'_i|} e'_i \cdot e_j \quad (3.19) \\ &= [\Delta] \cdot (e'_i \times e_j). \quad (3.20) \end{aligned}$$

Then we have $[\Delta] = \sum_k e_k \times e'_k$ as desired. □

With this equality, we can prove the Lefschetz fixed point theorem.

Proof. By previous lemmas, we have

$$\begin{aligned} [\Gamma(f)] \cdot [\Delta] &= [\Gamma(f)] \cdot \sum_k e_k \times e'_k \quad (3.21) \\ &= \sum_k (-1)^{|e_k|} f_* e_k \cdot e'_k \quad (3.22) \\ &= \sum_i (-1)^i Tr(f_* : H_i(X) \to H_i(X)). \quad (3.23) \end{aligned}$$

□

4. Fixed points of Frobenius map and counting points

Suppose we want to count the number of solutions of $y^2 = x^3 + x$ for $x, y \in \mathbb{F}_q$. The problem is that since the field is finite, the set of solutions is also finite and thus does not have a nice geometric structure.

An analogue is to solve the equation in the algebraic closure $\overline{\mathbb{F}_q} = \cup_n \mathbb{F}_{q^n}$. Let X be the set of solutions (x, y) of $y^2 = x^3 + x$ for $x, y \in \overline{\mathbb{F}_q}$. Given any $(x, y) \in X$,we have $(x^q, y^q) \in X$ since

$$(y^q)^2 = (x^3 + x)^q = (x^q)^3 + x^q, \tag{4.1}$$

which follows from the binomial theorem and the fact that $q = 0$ in $\mathbb{F}_q$.

The condition $(x, y) \in \mathbb{F}_q \times \mathbb{F}_q$ is equivalent to $(x^q, y^q) = (x, y)$. Let $f : X \to X$ be the map sending (x, y) to (x^q, y^q). Then the number of solutions for $x, y \in \mathbb{F}_q$ is just the number of fixed points of $Frob$.

Suppose that we have some cohomology theory $"H"^i$ in this geometry X and we have the Lefschetz fixed point theorem with respect to this cohomology theory. We know that

$$L(f) = \sum_i (-1)^i Tr(f_* : "H"^i(X) \to H^i(X)). \tag{4.2}$$

If we further assume that Betti numbers as well as traces of f_* are the same over $\overline{\mathbb{F}_{||}}$ and $\mathbb{C}$ for any general map f that can be described by polynomials with integer coefficients, then sometimes we can compute number solutions using complex geometry.

To proceed, we need the following three propositions. Let Λ be the lattice $\langle 1, i \rangle$ in the complex plane and let $E(\mathbb{C})$ denote solutions of the equation in $\mathbb{C}$. We know that multiplication by any $c \in \Lambda$ gives an endomorphism $f : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda$ and the following proposition shows that in fact any holomophic map is of this form.

Proposition 4.3. *Any holomorphic map $f : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda$ such that $f(0) = 0$ is given by multiplication by some $c \in \Lambda$, and thus the set of endomorphisms of $\mathbb{C}/\Lambda$ is $\mathbb{Z}[i]$.*

Proposition 4.4. *Holomorphic maps from $E(\mathbb{C})$ to $E(\mathbb{C})$ are all algebraic maps. i.e. $c \in \mathbb{Z}[i]$ gives a map from $E(\mathbb{C})$ to $E(\mathbb{C})$, which sends (x, y) to $(f(x, y), g(x, y))$ with $f, g \in \mathbb{Z}[i, 1/2][x, y]$.*

We also need the following proposition to lift the Frobenius map to $\mathbb{C}$.

Proposition 4.5. *If q is a prime power and $q \equiv 1 \bmod 4$, there exists $c \in \mathbb{Z}[i]$ such that $\|c\|^2 = q$ and multiplication by c is the endomorphism which lifts the Frobenius map.*

These three propositions can be proved using knowledge of algebraic geometry and elliptic curves but the complete proof is beyond the scope of this paper.

With these propositions, we can lift the Frobenius map to $\mathbb{C}$ and calculate the Lefschetz number. Let multiplication by $c \in \mathbb{Z}[i]$ denote the lifting of Frobenius map, call it F. We first look at the degree of this map.

The degree of the map $F : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda$ is the number of preimages of a class $[z] \in \mathbb{C}/\Lambda$. We calculate the number of preimages of 0, and let $x + yi$ be a preimage of 0, we have:

$$c \cdot (x + yi) = 0 + \lambda, \tag{4.6}$$

where $\lambda \in \Lambda$. There are q preimages and thuswe know that the degree is $\|c\|^2$. Since we also have $\|c\|^2 = q$ by the third proposition, we know degree of F is q. Hence

$$Tr(F_* : H_2(E(\mathbb{C})) \to H_2(E(\mathbb{C}))) = q. \tag{4.7}$$

Then we look at trace of F_* on $H_1(E(\mathbb{C}))$. In this case, F_* is the linear operator represented by the matrix $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$ where a is the real part of c and b is the imaginary part. Then the trace of F_* is simply $2a$. Further, we know that

$$2a \leq 2\|c\| = 2\sqrt{q}. \tag{4.8}$$

Since we assume that the Betti numbers as well as the traces of f_* are the same over $\mathbb{F}_q$ and $\mathbb{C}$, the Lefschetz number of the Frobenius map in $\bar{\mathbb{F}}_q$ equals the Lefschetz number of the lifting F in $\mathbb{C}$. Then we have

$$L(\text{Frob}) = L(F) = \sum_i (-1)^i Tr(F_* : H_i(E(\mathbb{C}))) = q - 2d\sqrt{q} + 1, \tag{4.9}$$

where $|d| = |a/\sqrt{q}| \leq 1$. And thus the number of solutions of the equation in $\mathbb{F}_q$ is just the number of fixed points of the Frobenius map, which is $q - 2d\sqrt{q} + 1$.

This result is consistent of our computation earlier in Example 1.5 since the coefficient of $q^{1/2}$ has absolute value less than or equal to 2. By using Lefschetz fixed point theorem as well as other tools in complex analysis and algebraic topology, we partially explained why the number of points in $\mathbb{F}_q$ on this curve looks almost like a polynomial function in q.

References

[1] Victor Guillemin and Allan Pollack. Differential Topology. American Mathematical Society. 2010.

[2] Allen Hatcher. Algebraic Topology. http://www.math.cornell.edu/ hatcher/AT/AT.pdf.

[3] Elias M. Stein and Rami Shakarchi. Complex Analysis. Princeton University Press. 2005.

[4] Andrew Sutherland. Elliptic Curves Lecture Notes. http://ocw.mit.edu/courses/mathematics/18-783-elliptic-curves-spring-2013/lecture-notes/MIT18_783S13_lec17.pdf.