

# The Weil Conjectures

Kevin Crooks

2009

## Contents

<b>1</b>	<b>An Introduction</b>	<b>2</b>
1.1	Background . . . . .	2
1.2	Statement of the conjectures . . . . .	2
<b>2</b>	<b>Projective Spaces</b>	<b>3</b>
2.1	Setting up the problem . . . . .	4
2.2	Proving for $\mathbb{P}^1$ . . . . .	5
2.3	Proof for general $\mathbb{P}^n(\mathbb{F}_q)$ . . . . .	6
<b>3</b>	<b>Betti Numbers</b>	<b>7</b>
<b>4</b>	<b>Quadratic Forms over <math>\mathbb{F}_q</math></b>	<b>10</b>
4.1	Introduction to Quadratic Forms . . . . .	10
4.2	Number of Solutions for a Quadratic Form . . . . .	12
<b>5</b>	<b>Extension</b>	<b>15</b>

# 1 An Introduction

## 1.1 Background

One application of the Weil conjectures is to study the number of integer solutions to the following problem:

$$f_i(x_1, x_2, \dots, x_n) = 0 \text{ for } i = 1, 2, \dots, r \quad (1)$$

Unfortunately, this problem can become very difficult to solve, very quickly. This is true, even if we only have  $r=1$ , that is when there is only one equation to solve. To simplify the problem, we can think of  $x_i$  as being elements of some finite field  $\mathbb{F}_q$ , where  $q$  is some prime power. In this case, we now look at the number of solutions modulo  $q$ .

If we let  $N_m$  be the number of solutions over the field  $q^m$ , we would like to be able to determine what this value is for various values of  $r$  and  $n$ .

Interestingly, the Weil conjectures make use of this idea, and extend it to claim more abstract properties of a function called the 'Zeta-Function'.

## 1.2 Statement of the conjectures

For this we aim to give an accurate statement of the conjectures, before explaining the meaning of the terms, and how they will apply to the special cases we will prove.

The following was derived by restricting the zeta-function to finite fields:

**Definition 1.1.** *Define the zeta function for a non-singular projective algebraic variety over a finite field  $\mathbb{F}_q$  where  $q = p^f$  (some prime  $p$ ) by:*

$$\zeta(X/\mathbb{F}_q, s) := \exp \left( \sum_{m=1}^{\infty} \frac{N_m}{m} (q^{-s})^m \right) \quad (2)$$

And  $N_m$  is the number of points defined in the 'degree  $m$  extension' of the projective algebraic variety.

It is worth noting that E. Freitag and R. Kiehl [3] give a slightly different definition for  $\zeta(X/\mathbb{F}_q, s)$  where  $\zeta(X/\mathbb{F}_q, s) =: f(s)$  (shorthand) is defined as follows:

$$f(0) = 1$$
$$\frac{f'(s)}{f(s)} = \sum_{m=1}^{\infty} N_m s^{m-1} \quad (3)$$

Unfortunately a lot of these terms are difficult to describe, but we will try! For more on this see J.W.P Hirschfeld [9]

A *projective algebraic variety* is a subset of  $\mathbb{P}^n$  and has some notion of zero. For example in a later chapter, we will want to find the number of solutions to  $ax^2 + by^2 = 0$  in a finite field. We also require that this subset is irreducible, so

in the above case, we don't want any factors of the polynomial in our field. The definition of *non-singular* is also not at all obvious. Hirschfeld gives the definition that a variety is non-singular if it does not have a singular point. Intuitively, a singular point on a curve for example would be a point where it self-intersects. For example the digit '8' as a curve, is singular, whereas the curve '0' is non-singular.

We will now give a justification of why definitions (2) and (3) could be expected to be equivalent (which they are). Suppose that we know that the solution series,  $f(s)$  is unique. Then as a trial solution, let  $f(s) = A \exp\left(\sum_{m=1}^{\infty} \frac{N_m}{m} s^m\right)$ , for some constant  $A$ . Now define  $g(s) := \sum_{m=1}^{\infty} \frac{N_m}{m} s^m$ . Then for  $f(s)$  to make sense,  $g(s)$  must be finite and so absolutely convergent (as all terms are positive). This means we can differentiate  $g(s)$  termwise:

$$f'(s) = g'(s)f(s) = \left(\sum_{m=1}^{\infty} N_m s^{m-1}\right) f(s)$$

And so  $\frac{f'(s)}{f(s)} = g'(s)$  which is as in equation (2). The initial condition shows that  $A = 1$ .

We are now ready to give the statement of the Weil Conjectures:

**Definition 1.2.** [1, 2, 3]

1.  $\zeta(X/\mathbb{F}_q, s)$  is rational and can be written in the form:

$$\zeta(X/\mathbb{F}_q, s) = \frac{P_1(T)P_3(T)\dots P_{2n-1}(T)}{P_0(T)P_2(T)\dots P_{2n}(T)}$$

Where  $T := q^{-s}$  and  $n = \dim(X)$ .

2.  $P_{2i}(T) = (1 - q^i T)$ . And;

$$P_{2i-1}(T) = \prod_j (1 - \alpha_{i,j} T)$$

Furthermore, in both cases if  $\lambda$  is a root of  $P_i$ , then  $|\frac{1}{\lambda}| = q^{\frac{i}{2}}$ .

3. If  $X$  is a "good reduction from a complex algebraic variety  $\tilde{X}$ , then the degree of  $P_i(t)$  is equal to the  $i$ -th Betti number of  $\tilde{X}$ .
4. There is a functional equation for  $\zeta(X/\mathbb{F}_q, s)$ .

In this essay we will focus mainly on assertions (1) and (2) and briefly show case (3) for projective space, but (4) is stated merely for completion.

## 2 Projective Spaces

In this section we will prove the first two parts of the Weil Conjectures, for projective space over a finite field. Firstly, we need to say what this means.

## 2.1 Setting up the problem

**Definition 2.1.** Define an equivalence relation  $\sim$  on  $\mathbb{F}^{n+1}$  by  $(x_0, \dots, x_n) \sim (y_0, \dots, y_n)$  if  $(x_0, \dots, x_n) = \lambda(y_0, \dots, y_n)$  some  $\lambda \in \mathbb{F}^*$

**Definition 2.2.** The projective space  $\mathbb{P}^n(\mathbb{F}) := (\mathbb{F}^{n+1} \setminus \{0\}) / \sim$ , where  $\sim$  is as defined in 2.1.

**Lemma 2.3.** for  $0 \neq x \in \mathbb{F}_p$  where  $p$  is prime, then  $n \in \mathbb{N}$ ,  $nx = 0 \implies n = kp$ , for some  $k \in \mathbb{N}$ .

*Proof.*  $\mathbb{F}_p$  forms a group under addition modulo  $p$ . The order of each element in  $\mathbb{F}_p$  must divide the order of the group, which is  $p$ . As  $p$  is prime, the order of every non zero element is  $p$ . Therefore,  $x \neq 0$  and  $nx = 0$  implies  $n$  is a multiple of  $p$ , i.e  $n = kp$  some  $k \in \mathbb{N}$ .  $\square$

**Corollary 2.4.** Fix  $0 \neq x \in \mathbb{F}_p$ , then for any  $0 \neq n \in \mathbb{F}_p$ ,  $nx \neq 0$ .

This just follows from the fact that  $n$  is less than  $p$ .

**Lemma 2.5.** If  $\mathbb{F}_p$  is a finite field with  $p$  elements and  $p$  prime,  $\mathbb{P}^n(\mathbb{F}_p)$  has  $p^n + p^{n-1} + \dots + p + 1$  elements.

*Proof.*  $\mathbb{F}_p^*$  has  $(p - 1)$  elements so each equivalence class can have at most  $p - 1$  elements. By 2.4, it has exactly  $p - 1$  elements. The number of choices of  $(x_0, \dots, x_n)$  in  $\mathbb{F}^{n+1}$  is  $p^{n+1} - 1$  (the zero point). So the total number of equivalence classes is:

$$\frac{p^{n+1} - 1}{p - 1} = 1 + p + \dots + p^{n-1} + p^n$$

$\square$

Now we will extend the idea of a finite field over  $p$ , where  $p$  is prime to a finite field over  $q$ , where  $q$  is some prime power.

**Proposition 2.6.** For a finite field  $\mathbb{F}_q$ , where  $q$  is some prime power,  $\mathbb{P}^n(\mathbb{F}_q)$  has  $q^n + q^{n-1} + \dots + q + 1$  elements.

*Proof.* Using the same proof as 2.5, it is sufficient to show that each equivalence class has exactly  $q - 1$  elements. By definition, each equivalence class has at most  $q - 1$  elements. To show they have exactly this many, note that  $\mathbb{F}_q$  is a 1-dimensional vector space (as  $\mathbb{F}_q$  is a field). so we get the same result as in 2.4: Fix  $v \in \mathbb{F}_q$  then for any non-zero  $\alpha, \beta \in \mathbb{F}_q$ ,  $\alpha v = \beta v \iff (\alpha - \beta)v = 0 \iff (\alpha - \beta) = 0$ , as  $(\alpha - \beta)^{-1}$  exists. Then, in the same way, the number of elements in  $\mathbb{P}^n(\mathbb{F}_q)$  is

$$\frac{q^{n+1} - 1}{q - 1} = 1 + q + \dots + q^{n-1} + q^n$$

$\square$

This is all that is needed to determine the value of  $N_m$  for projective space over a finite field. For this, we note that the ‘degree  $m$  extension’ over a finite field  $\mathbb{F}_q$  is simply the finite field  $\mathbb{F}_{q^m}$ . So the value of  $N_m$  is easily deduced from the previous propositions, but is important, so will be stated as the theorem for this section:

**Theorem 2.7.** *The number of elements,  $N_m$  defined in the degree  $m$  extension of the projective algebraic variety,  $\mathbb{F}_q$ , is given by:*

$$N_m = \frac{q^{m(n+1)} - 1}{q^m - 1}$$

*Proof.* substitute  $q^m$  into 2.6. □

## 2.2 Proving for $\mathbb{P}^1$

By the previous section, we know that, in the formula for  $\zeta(X/\mathbb{F}_q, s)$ :

$$N_m = \frac{q^{m(n+1)} - 1}{q^m - 1}$$

In the case for  $\mathbb{P}^1$ , we have that  $n = 1$  so we just get  $1 + q^m$ . This allows us to reach the following conclusion:

**Proposition 2.8.** *Let  $X$  be projective 1-space over a finite field  $\mathbb{F}_q$  (some prime power  $q$ ), then:*

- $\zeta(X/\mathbb{F}_q, s)$  is rational and;
- $\zeta(X/\mathbb{F}_q, s) = \frac{1}{(1-q^{-s})(1-q^{1-s})}$ .

*Proof.*

$$\begin{aligned} \zeta(X/\mathbb{F}_q, s) &= \exp\left(\sum_{m=1}^{\infty} \frac{N_m}{m} (q^{-s})^m\right) = \exp\left(\sum_{m=1}^{\infty} \frac{1+q^m}{m} (q^{-s})^m\right) \\ &= \exp\left(\sum_{m=1}^{\infty} \frac{q^{m-ms}}{m} + \sum_{m=1}^{\infty} \frac{(q^{-s})^m}{m}\right) \end{aligned}$$

Now note that:

$$\sum_{m=1}^{\infty} \frac{t^m}{m} = \log\left(\frac{1}{1-t}\right) \tag{4}$$

for  $|t| \leq 1$  and  $t \neq 1$ . And letting  $t = q^{-s}$  and  $t = q^{1-s}$  in the respective components of the sums produces:

$$\begin{aligned} \zeta(X/\mathbb{F}_q, s) &= \exp\left[\log\left(\frac{1}{1-q^{1-s}}\right) + \log\left(\frac{1}{1-q^{-s}}\right)\right] \\ &= \exp\left[\log\left(\frac{1}{(1-q^{1-s})(1-q^{-s})}\right)\right] = \frac{1}{(1-q^{-s})(1-q^{1-s})} \end{aligned}$$

□

The following Corollary proves conjectures 1 and 2 for  $\mathbb{P}^1$ :

**Corollary 2.9.**  $\zeta(X/\mathbb{F}_q, s) = \frac{P_1(T)}{P_0(T)P_2(T)}$  where  $P_{2i-1} = \prod_j (1 - \alpha_{i,j}T)$ , and  $P_{2i}(T) = (1 - q^i T)$ , for  $0 \leq i \leq 1$  and  $|\frac{1}{\lambda}| = q^{\frac{i}{2}}$  for  $\lambda$  a root of  $P_i$ .

*Proof.* 1.

$$P_1(T) = \prod_{j=0}^{j=0} (1 - \alpha_{1,j}T) = 1$$

and the fact  $|\frac{1}{\lambda}| = q^{\frac{i}{2}} \forall$  roots  $\lambda$  is trivially true, as there are no such  $\lambda$ .

2.

$$P_0(T) = (1 - q^{-s}) = (1 - 1.T)$$

so  $|\frac{1}{\lambda}| = 1 = q^0$ .

3.

$$P_2(T) = (1 - q^{1-s}) = (1 - q.T) \text{ so } |\frac{1}{\lambda}| = q^1 = q^{\frac{2}{2}}.$$

□

### 2.3 Proof for general $\mathbb{P}^n(\mathbb{F}_q)$

. Although the proof of this is very similar to the previous case, the arguments were easier to see in the above simple case, and so the complete proof for  $\mathbb{P}^n$  is clearer.

**Proposition 2.10.** *Let  $X$  be a projective  $n$ -space over a finite field  $\mathbb{F}_q$ , then:*

1.  $\zeta(X/\mathbb{F}_q, s)$  is rational and;

2.  $\zeta(X/\mathbb{F}_q, s) = \frac{1}{(1-T)(1-qT)\dots(1-q^nT)}$

*Proof.* Recall that  $N_m = \frac{q^{m(n+1)} - 1}{q^m - 1} = 1 + q^m + \dots + q^{m(n-1)} + q^{mn}$

$$\begin{aligned} \zeta(X/\mathbb{F}_q, s) &= \exp\left(\sum_{m=1}^{\infty} \frac{N_m}{m} (q^{-s})^m\right) = \exp\left(\sum_{m=1}^{\infty} \frac{1 + q^m + \dots + q^{m(n-1)} + q^{mn}}{m} (q^{-s})^m\right) \\ &= \exp\left(\sum_{m=1}^{\infty} \frac{(q^{-s})^m + (q^{1-s})^m + \dots + (q^{(n-1)-s})^m + (q^{n-s})^m}{m}\right) \end{aligned}$$

From this we can separate the sums and use (4), to get the required result: (See back to proof of 2.8)

$$\zeta(X/\mathbb{F}_q, s) = \frac{1}{(1 - q^{-s})(1 - q^{1-s})\dots(1 - q^{n-s})} \quad (5)$$

□

Again, following the method of section 2.1...

**Theorem 2.11.**  $\mathbb{P}^n(\mathbb{F}_q)$  satisfies conditions 1 and 2 of the Weil Conjectures.

*Proof.* Because of the previous section, it is sufficient to prove that:

$P_{2i} = (1 - q^i T)$  and  $|\frac{1}{\lambda}| = q^{\frac{i}{2}}$ , for each  $\lambda$  a root of  $P_i$ .

By Equation (4) it is clear that for even  $i$ ,  $P_i = (1 - q^{\frac{i}{2}-s}) = (1 - q^{\frac{i}{2}} q^{-s})$ . And so  $|\frac{1}{\lambda}| = q^{\frac{i}{2}}$ , as required.  $\square$

It is true that all the conjectures can be proven for  $\mathbb{P}^n(\mathbb{F}_q)$ , however we will leave out condition 4. We will now show (roughly) that condition 3 is also satisfied. However, this requires a chapter of its own!

### 3 Betti Numbers

The concept of Betti numbers is very complicated but we will try to define, at least intuitively, what they are. Although deriving the Betti numbers for  $\mathbb{P}^n(\mathbb{F}_q)$  is too difficult, we will follow along in parallel with a simpler example.

The idea of a Betti number comes from trying to consider a fundamental property of a topological space. We know that there is a difference between a sphere and a torus for example (namely, one has a ‘hole’ in it). To make this more rigorous, we can consider how many times we can ‘cut’ the object, while still keeping it in one piece.

It is clear that making any cut on the sphere will separate it into two pieces. However, if we cut a torus cleverly (from the outside to the hole), it will stay in one piece.

The Betti numbers exploit this fact. In order to define what a Betti number is, we must first start with the following:

**Definition 3.1.** [6] A Chain complex or Chain space is a sequence of abelian groups:

$$\dots C_{n+1} \xrightarrow{\partial_{n+1}} C_n \xrightarrow{\partial_n} C_{n-1} \rightarrow \dots \rightarrow C_1 \xrightarrow{\partial_1} C_0 \xrightarrow{\partial_0} C_{-1} \rightarrow \dots$$

where each  $\partial_i$  is a homomorphism from  $C_i$  to  $C_{i-1}$ , such that the image of one map is contained in the kernel of the next. That is,  $(\partial_{n-1}) \circ (\partial_n) = 0 \forall n$ .

We won’t worry too much about how to construct these groups except to say that it can be done! Before defining what the Betti numbers are, we require another technical definition:

**Definition 3.2.** Define the  $n$ -th homology group,  $H_n(X)$  of  $X$  to be the quotient group:

$$H_n(X) = \frac{\text{Ker}(d_n)}{\text{Im}(d_{n+1})}$$

Notice that this makes sense since by 3.1,  $\text{Im}(d_{n+1}) \subset \text{Ker}(d_n)$ . From this, we are now ready to define Betti numbers:

**Definition 3.3.** The  $i$ -th Betti number,  $b_i(X)$ , of  $X$  is defined to be  $b_i(X) := \text{Rank}(H_i(X))$ .

At this point, we will do a very simple example to show the ideas defined above. We should mention that there are many different ways to calculate the homology groups of a space, partly depending on the space being considered. A. Grothendieck used ‘etale cohomology’, but one of the simpler techniques (for simple spaces) is to consider  $n$ -simplices. These are the  $n$ -dimensional equivalent of a triangle, tetrahedron etc. It turns out that we can consider the *boundary maps* of these. This essentially means that for the triangle we consider its edges, and for the edges we consider the endpoints (the vertices of the triangle).

**Example 3.4.** (See Hatcher [7]) Consider  $S^1$ . Then we can think of a point,  $v$ , on the circle as being a 0-simplex, and the path connecting this vertex to itself,  $e$ , as a 1-simplex. Clearly there are no simplices in dimensions higher than 2. Then the boundary map  $\partial_1(e) = v - v = 0$ , since  $e$  is a loop from  $v$  to itself. Also  $\partial_0(v) = 0$  since this is the 0-simplex. And so we get the following chain complex:

$$0 \xrightarrow{\partial_2} C_1 \xrightarrow{\partial_1} C_0 \xrightarrow{\partial_0} 0$$

And we get that  $\text{Ker}(\partial_1) = C_1 \cong \mathbb{Z}$  (since  $C_1$  is generated by  $e$ ). And since  $\text{Im}(\partial_2) = 0$  we get that  $H_1 \cong \mathbb{Z}$ . Similarly,  $\text{Ker}(\partial_0) = C_0 \cong \mathbb{Z}$  and  $\text{Im}(\partial_1) = 0$  and so  $H_0 \cong \mathbb{Z}$ . And therefore, the Betti numbers for  $S^1$  are:

$$b_i = \text{Rank}(H_i) = \begin{cases} \text{Rank}(\mathbb{Z}) = 1 & \text{if } i = 0 \text{ or } i = 1 \\ 0 & \text{else} \end{cases}$$

So this is the general idea for calculating the homology groups and also the Betti numbers. In more complex examples it becomes extremely difficult to use this method, and so other techniques are required. Another (equivalent) method is *singular homology*, which is also discussed by Hatcher [7]. However, instead of doing this, we will look at the slightly more complicated example of using simplicial homology to calculate the Betti numbers for a 2-torus. The idea behind finding the Betti numbers should be clearer, and we can then state the result for  $\mathbb{P}^n(\mathbb{F}_q)$ .

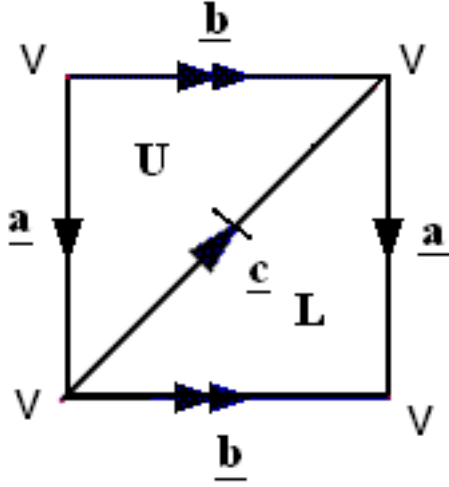


Figure 1: 2-Torus

**Example 3.5.** See Fig.1 for a diagram of the 2-torus. We can split this up into two 2-simplices;  $U$  and  $L$ . In a similar way to the previous example,  $\partial_1(v) = 0$  for all  $a, b, c$ , since all begin and end on  $v$ . We can also see that  $\partial_2(U) = a - b + c$  and  $\partial_2(L) = a - b + c$ . So we get the chain complex:

$$0 \xrightarrow{\partial_3} C_2 \xrightarrow{\partial_2} C_1 \xrightarrow{\partial_1} C_0 \xrightarrow{\partial_0} 0$$

Then we find the Homology groups:

- $H_0$ :  $H_0 = \text{Ker}(\partial_0)/\text{Im}(\partial_1) = \text{Ker}(\partial_0) \cong \mathbb{Z}$ , since  $\text{Im}(\partial_1) = 0$ .
- $H_1$ : We can write a basis for  $C_1$  like  $\{a, b, a+b-c\}$ . And we know that all elements of  $C_1$  are in its Kernel. Since a basis for  $\text{Im}(\partial_2)$  is  $\{a+b-c\}$ , we see that  $H_1 = \text{Ker}(C_1)/\text{Im}(C_2) \cong \mathbb{Z}^2$ .
- $H_2$ :  $\partial_2(U) = \partial_2(L)$ , and so  $U-L$  is in the Kernel of  $\partial_2$ . Since  $\text{Rank}(\partial_2) = 2$  and  $\text{Im}(\partial_2)$  is spanned by  $\{a+b-c\}$ , it must be the case that  $\{U-L\}$  spans  $\text{Im}(\partial_2)$ . Therefore  $H_2 = \text{Ker}(\partial_2)/\text{Im}(\partial_3) = \text{Ker}(\partial_2) \cong \mathbb{Z}$ .

And so the Betti numbers for the 2-torus are:

$$b_i = \begin{cases} 1 & \text{if } i = 0 \text{ or } i = 2 \\ 2 & \text{if } i = 1 \\ 0 & \text{else} \end{cases}$$

So now that we have defined what a Betti number is, it is possible to find the Betti numbers for  $\mathbb{P}^n(\mathbb{F}_q)$ . Because this is so difficult, it will be stated without proof.

**Theorem 3.6.** *The Betti numbers for  $\tilde{X}$  where  $X = \mathbb{P}^n(\mathbb{F}_q)$  are:*

$$b_i = \begin{cases} 1 & \text{If } i = 2k \\ 0 & \text{If } i = 2k - 1 \end{cases} \quad \text{some } k \in \mathbb{N} \quad (6)$$

And in particular:

**Theorem 3.7.** *Condition 3 of the conjectures are satisfied.*

*Proof.* By 2.10, we have for  $\mathbb{P}^n(\mathbb{F}_q)$ :

$$P_i = \begin{cases} (1 - q^{\frac{i}{2}}T) & \text{If } i = 2k \\ 1 & \text{If } i = 2k - 1 \end{cases} \quad \text{some } k \in \mathbb{N}$$

And so,

$$\text{deg}(P_i) = \begin{cases} 1 & \text{If } i = 2k \\ 0 & \text{If } i = 2k - 1 \end{cases} = b_i \text{ some } k \in \mathbb{N}$$

□

This concludes the section showing the conjectures for projective space. In the next section, we will extend this idea to a more complex case:

## 4 Quadratic Forms over $\mathbb{F}_q$

(Most of this chapter by R.Lidl and H.Niederreiter [8]). This case corresponds to when we have a system of one equation ( $r=1$ ) and the degree of the polynomial is at most 2. This is to say, we have a quadratic form over a finite field. We now want to ask, how many solutions does this equation have in a field  $\mathbb{F}_q$ ? (we will assume that  $q$  is odd).

Before we start this, we need a few definitions:

### 4.1 Introduction to Quadratic Forms

**Definition 4.1.** *The quadratic character,  $\eta(c)$ , some  $c \in \mathbb{F}_q$  is defined as:*

$$\eta(c) = \begin{cases} 0, & \text{if } c = 0 \\ +1, & \text{if } c = x^2, \text{ some } x \in \mathbb{F}_q^* \\ -1, & \text{else} \end{cases}$$

*Notes:*

- In projective space we will always work in  $\mathbb{F}_q^*$  and so  $\eta(c)$  is always non-zero.
- We will also use (without proof) that an equivalent definition is:

$$\eta(c) = c^{\frac{q-1}{2}} \pmod{q}$$

More detail on this is found in Lidl and Niederreiter [8], essentially, this is useful when studying quadratic forms because it identifies the elements which are perfect squares.

**Lemma 4.2.**  $\eta(a)\eta(b) = \eta(ab) \forall a, b \in \mathbb{F}_q$

*Proof.*  $\eta(a)\eta(b) = a^{\frac{q-1}{2}}b^{\frac{q-1}{2}} = (ab)^{\frac{q-1}{2}} = \eta(ab)$ . □

Which gives the following useful corollary:

**Corollary 4.3.**  $\eta(a) = \eta(a^{-1}) \forall a \in \mathbb{F}_q^*$

*Proof.*  $1 = \eta(1) = \eta(aa^{-1}) = \eta(a)\eta(a^{-1})$ , and so they have the same sign. □

The next definition isn't very useful for what we are doing, since we are looking at the solutions to  $f(x_1, x_2, \dots, x_n) = b$  for  $b = 0$ , but most of the results generalise for any  $b \in \mathbb{F}_q$ .

**Definition 4.4.** *The integer-valued function  $v(b)$  for  $b \in \mathbb{F}_q$  is:*

$$v(b) = \begin{cases} q-1, & \text{if } b = 0 \\ -1, & \text{if } b \neq 0 \end{cases}$$

One more definition before we move on to some theorems!

**Definition 4.5.** *let  $A$  be the matrix corresponding to the quadratic form for the polynomial  $f$ . Then  $\det(f) := \det(A)$ , and  $f$  is said to be non-degenerate if  $\det(f) \neq 0$ .*

As a rule for notation,  $N(f(x_1, x_2, \dots, x_n) = b)$  is the number of solutions to the equation. Before demonstrating the idea behind finding the number of solutions to such an equation, we will need the following fact:

**Lemma 4.6.** *For  $a \in \mathbb{F}_q$ , we have that the number,  $N(a)$ , of solutions to  $x^2 = a$  is given by:*

$$N(a) = \begin{cases} 2 & \text{if } a \neq 0 \text{ and } x^2 = a \text{ some } x \in \mathbb{F}_q^* \\ 1 & \text{if } a = 0 \\ 0 & \text{else} \end{cases}$$

A particularly useful result of 4.6 is that  $N(a) = 1 + \eta(a)$ .

Now we are nearly ready to start counting the number of solutions, but we first require the following formulae (for proof of these see Lidl and Niederreiter [8]).

**Proposition 4.7.** *let  $f(x) = a_2x^2 + a_1x + a_0 \in \mathbb{F}_q[x]$  for  $q$  odd,  $a_2 \neq 0$ . Then*

$$\sum_{c \in \mathbb{F}_q} \eta(f(c)) = \nu(d)\eta(a_2)$$

Where  $d = a_1^2 - 4a_0a_2$ .

**Proposition 4.8.**

$$\sum_{c_1+\dots+c_m=b} \nu(c_1)\dots\nu(c_k) = \begin{cases} \nu(b)q^{m-1} & \text{if } k = m \\ 0 & \text{else} \end{cases}$$

Now that we have these results, we are ready to find the value of  $N_m$  in the case of quadratic forms.

## 4.2 Number of Solutions for a Quadratic Form

We will start straight away with a critical Proposition:

**Proposition 4.9.** ([8]) *If  $q$  is odd, and for any  $b \in \mathbb{F}_q$ ,  $a_1, a_2 \in \mathbb{F}_q^*$ , we have that:*

$$N(a_1x_1^2 + a_2x_2^2 = b) = q + \nu(b)\eta(-a_1a_2)$$

*Proof.* By a simple counting argument,

$$N(a_1x_1^2 + a_2x_2^2 = b) = \sum_{c_1+c_2=b} N(a_1x_1^2 = c_1)N(a_2x_2^2 = c_2)$$

So in each case, we want to know if  $c_ia_i^{-1}$  is a square of an element in  $\mathbb{F}_q$ . By 4.6, we know that if it is, then provided  $c_ia_i^{-1} \neq 0$ , we must have exactly 2 solutions. Therefore this is equal to:

$$= \sum_{c_1+c_2=b} (1 + \eta(c_1a_1^{-1}))(1 + \eta(c_2a_2^{-1}))$$

From 4.2 and 4.3 we get:

$$= q + \eta(a_1) \sum_{c_1 \in \mathbb{F}_q} \eta(c_1) + \eta(a_2) \sum_{c_2 \in \mathbb{F}_q} \eta(c_2) + \eta(a_1a_2) \sum_{c_1+c_2=b} \eta(c_1c_2)$$

But note that the second and third terms sum to zero:

$$= q + \eta(a_1a_2) \sum_{c \in \mathbb{F}_q} \eta(bc - c^2)$$

Where we use the substitution  $c_2 = b - c_1$  and let  $c_1$  vary over  $\mathbb{F}_q$ . Finally we use 4.7 and the fact that  $a_0 = 0 \iff d = a_1^2 \iff \nu(d) = \nu(a_1)$ , to give the expression equal to:

$$q + \eta(a_1a_2)\nu(b)\eta(-1) = q + \nu(b)\eta(-a_1a_2)$$

□

Using this proposition, we can give a general formula for a quadratic in  $n$  variables. There is a different formula for even and odd  $n$ . We will give the proof for  $n$  even, and state the result for  $n$  odd. This is because the proofs are fairly similar, and it is not necessary to repeat it.

**Theorem 4.10.** *Let  $f$  be a quadratic in  $n = 2m$ ,  $m \in \mathbb{N}$ , over  $\mathbb{F}_q$ . And  $b \in \mathbb{F}_q$ . Then*

$$N(f(x_1, x_2, \dots, x_n) = b) = q^{n-1} + \nu(b)q^{\frac{n-2}{2}}\eta((-1)^{\frac{n}{2}}a_1 \dots a_n)$$

Where  $a_i$  are the coefficients of  $x_i$  in  $f$

*Proof.* We will use the result that any quadratic can be rewritten in the form  $a_1x_1 + a_2x_2 + \dots + a_nx_m$ ,  $a_i \in \mathbb{F}_q$ , such that the number of solutions does not change. Then by a similar argument for 2 variables:

$$N(f(x_1, x_2, \dots, x_n) = b) = \sum_{c_1 + \dots + c_m = b} N(a_1x_1^2 + a_2x_2^2 = c_1) \dots N(a_{n-1}x_{n-1}^2 + a_nx_n^2 = c_m)$$

And using 4.9:

$$= \sum_{c_1 + \dots + c_m = b} [q + \nu(c_1)\eta(-a_1a_2)] \dots [q + \nu(c_m)\eta(-a_{n-1}a_n)]$$

This expression initially looks like it will not easily simplify, but using 4.8, we see that any cross terms involving a  $\nu(c_i)$ , that does not contain *all* of them, goes to 0 under the sum. And so:

$$\sum_{c_1 + \dots + c_m = b} q^m + \nu(c_1) \dots \nu(c_m) \eta(-a_1a_2) \eta(-a_3a_4) \dots \eta(-a_{n-1}a_n)$$

By multiplicity of  $\eta$ , we can make the substitution:

$\eta(-a_1a_2)\eta(-a_3a_4)\dots\eta(-a_{n-1}a_n) = \eta((-1)^m a_1 \dots a_n)$ , which gives:

$$\begin{aligned} &= q^m \left( \sum_{c_1 + \dots + c_m = b} 1 \right) + \eta((-1)^m a_1 \dots a_n) \left( \sum_{c_1 + \dots + c_m = b} \nu(c_1) \dots \nu(c_m) \right) \\ &= q^m q^{m-1} + \eta((-1)^m a_1 \dots a_n) \sum_{c_1 + \dots + c_m = b} \nu(c_1) \dots \nu(c_m) \end{aligned}$$

Then using 4.8 again we get:

$$\begin{aligned} &= q^{2m-1} + \eta((-1)^m a_1 \dots a_n) \nu(b) q^{m-1} \\ &= q^{n-1} + \nu(b) q^{n-1} \eta((-1)^{\frac{n}{2}} a_1 \dots a_n) \end{aligned}$$

□

The proof for the case where  $n$  is odd has a similar method, so will not be proven in detail:

**Theorem 4.11.** *The analogue of 4.10 with*

$$N(f(x_1, \dots, x_n) = b) = q^{n-1} + q^{\frac{n-1}{2}} \eta((-1)^{\frac{n-1}{2}} b a_1 \dots a_n)$$

*Proof.* Similar to proof of 4.10 with the first line being as follows:

$$\sum_{c_1+c_2=b} N(a_1 x_1^2 = c_1) N(a_2 x_2^2 + \dots + a_n x_n^2 = c_2)$$

Using 4.7, gives the result.  $\square$

We will conclude by using the above theorems to show how the Zeta function can be calculated for a quadratic form:

**Example 4.12.** *For this example, we will take a general field  $\mathbb{F}_q$ , and for simplicity, take the case  $n = 2$ . Then apply 4.10, and letting  $b = 0$ , we get:*

$$N = q + \nu(0)q^0 \eta(-a_1 a_2)$$

And so:

$$N_m = q^m + (q^m - 1) \cdot 1 \cdot \eta(-a_1 a_2) \quad (7)$$

Then the Zeta-Function is as follows:

$$\begin{aligned} \zeta(X/\mathbb{F}_q, s) &= \exp \left( \sum_{m=1}^{\infty} \frac{q^m + (q^m - 1) \eta(-a_1 a_2)}{m} (q^{-s})^m \right) \\ &= \exp \left( \sum_{m=1}^{\infty} \frac{(q^{-s+1})^m}{m} + \eta(-a_1 a_2) \frac{(q^{-s+1})^m}{m} - \eta(-a_1 a_2) \frac{(q^{-s})^m}{m} \right) \end{aligned}$$

Using the same substitution as for projective space:

$$\zeta(X/\mathbb{F}_q, s) = \exp \left( \log \left( \frac{1}{1 - q^{-s+1}} \right) + \eta(-a_1 a_2) \log \left( \frac{1}{1 - q^{-s+1}} \right) - \eta(-a_1 a_2) \log \left( \frac{1}{1 - q^{-s}} \right) \right)$$

now use the substitution  $q^{-s} = T$ :

$$\zeta(X/\mathbb{F}_q, s) = \frac{(1 - T)^{\eta(-a_1 a_2)}}{(1 - qT)(1 - qT)^{\eta(-a_1 a_2)}} = \begin{cases} \frac{1}{(1 - qT)} & \text{if } \eta(-a_1 a_2) = 0 \\ \frac{(1 - T)}{(1 - qT)^2} & \text{if } \eta(-a_1 a_2) = 1 \\ \frac{1}{(1 - T)} & \text{if } \eta(-a_1 a_2) = -1 \end{cases}$$

## 5 Extension

Of course all the conjectures have now been proven for every case, but another example which is (relatively) easy to verify directly, is that of a projective curve over  $\mathbb{F}_q$ . We will state the result:

**Theorem 5.1.** (Hulsbergen [2]) *Let  $X$  be a non-singular projective curve over  $\mathbb{F}_q$ , then:*

$$\zeta(X/\mathbb{F}_q, s) = \frac{P(X/\mathbb{F}_q, s)}{(1 - q^{-s})(1 - qq^{-s})} \quad \text{with} \quad P(X/\mathbb{F}_q, s) = \prod_{i=1}^{2g} (1 - \alpha_i q^{-s})$$

Where  $|\alpha_i| = q^{\frac{1}{2}}$  and  $g$  is the genus of the curve.

Straight away we have this corollary:

**Corollary 5.2.** *All zeroes for  $\zeta(X/\mathbb{F}_q, s)$  lie on the line  $Re(s) = \frac{1}{2}$*

*Proof.* From 5.1, we know that the zeroes occur when  $q^{-s} = \alpha_i$  for some  $i$ . Write  $s = a + bi$  some  $a, b \in \mathbb{R}$ . Since  $|\alpha_i| = q^{\frac{1}{2}}$ , we have that:

$$q^{-s} = q^{-a-bi} = q^{-\frac{1}{2}} \iff q^{(\frac{1}{2}-a)-bi} = 1$$

Now write this in polar form, and  $Log(x)$  the principle logarithm:

$$q^{(\frac{1}{2}-a)-bi} = e^{[(\frac{1}{2}-a)-bi]Log(q)} = e^{(\frac{1}{2}-a)Log(q)} e^{i(-bLog(q))} = r e^{i\theta}$$

For  $r = e^{(\frac{1}{2}-a)Log(q)}$  and  $\theta = -bLog(q)$ . Then this is false if  $r \neq 1$ . So we must have:

$$e^{(\frac{1}{2}-a)Log(q)} = 1 \iff \frac{1}{2} - a = 0 \iff a = \frac{1}{2}$$

Since  $1 \neq q \in \mathbb{R}$ . And so  $Re(s) = a = \frac{1}{2}$ . □

The completed proof of these conjectures did not work on a case by case basis, but was done mainly using a branch of mathematics called etale-cohomology. A large part of this work was by A. Grothendieck. However, the final part of the conjectures to be proven was the analogue of the Riemann hypothesis for finite algebraic varieties. This was proven in 1973 by P. Deligne, which completed the proof of the Weil Conjectures, for which he was awarded a Fields medal in 1978.

## References

- [1] K. Ireland, M. Rosen A Classical Introduction to Modern Number Theory
- [2] W.W.J. Hulsbergen Conjectures in Arithmetic Algebraic Geometry
- [3] E. Freitag, R. Kiehl Etale Cohomology and the Weil Conjecture
- [4] M.Reid and B.Szendroi Geometry and Topology
- [5] N.Lauritzen Concrete Abstract Algebra
- [6] J. Roe Betti numbers
- [7] A. Hatcher Algebraic Topology
- [8] R.Lidl, H.Niederreiter Finite Fields
- [9] J.W.P Hirschfeld Projective Geometries over Finite Fields