ZETA FUNCTION FOR FERMAT HYPERSURFACES

RANDY MARTINEZ

Abstract. In this paper we find a way to compute the number of solutions to Fermat hypersurfaces over finite fields. This can be developed by first considering characters over these finite fields and introducing Gauss sums and Jacobi sums. Then we proceed with introducing the zeta function for hypersurfaces and showing some wonderful properties and results about it. We then put everything together to compute the number of points on these hypersurfaces and use this to compute the zeta function.

Contents

1. Introduction

Computing the number of points of objects is a fundamental problem in several areas of mathematics. Arithmetic geometry is a field where this issue is investigated in great detail, and our goal is to study the number of solutions of the equation

$$x^n + y^n + z^n = 0$$

over a finite field. We will investigate this in more generality by looking at Fermat hypersurfaces. Fermat hypersurfaces over a field F are subsets of projective n-space defined by equations of the form

$$x_1^m + x_2^m + ... + x_n^m = 0$$

from the ring of polynomials $F[x_1, ..., x_n]$. When F is a finite field, it makes sense to ask for the number of points in this set. We will take the approach using characters over $\mathbb{F}_q$ and the zeta function over hypersurfaces and follow Ireland and Rosen [2] closely while developing the theory needed.

2. Projective Hypersurfaces

2.1. Affine and Projective n-space.

Definition 2.1. Let F be a field and $A^n(F) = \{(a_1, ..., a_n) : a_i \in F\}$ be the n-tuples of elements in F. We call $A^n(F)$ the affine n-space over F.

Consider the set of points $A^{n+1} \setminus \{\mathbf{0}\}$, where $\mathbf{0}$ is the zero vector in $A^{n+1}(F)$. Let $a = (a_1, ..., a_{n+1})$ and $b = (b_1, ..., b_{n+1})$ and define the equivalence relation:

$$a \sim b \text{ if there exists } c \in F^\times \text{ such that } a_i = cb_i \text{ for all i.}$$

This is an equivalence relation because of the fact that the units of F form a group under multiplication.

Definition 2.2. The set of equivalence classes is called projective n-space over F and is denoted $P^n(F)$.

In the case where F is a finite field of order q, it is easy to see that $|A^n(F)| = q^n$. In the construction of $P^n(F)$ we started with $q^{n+1}-1$ points from $A^{n+1}\setminus\{\mathbf{0}\}$, and there are $|F^\times| = q-1$ points in an equivalence class, which gives us that $|P^n(F)| = \frac{q^{n+1}-1}{q-1} = q^n + q^{n-1} + ... + q + 1$. Now let $a = (a_0, a_1, ..., a_n)$ and consider the subset of $P^n(F)$ where the first coordinate is zero: $H := \{[a] \in P^n(F) : a_0 = 0\}$. H is known as the hyperplane at infinity. Notice that H has the structure of $P^{n-1}(F)$.

Proposition 2.1. $\Phi : P^n(F) \setminus H \to A^n, \Phi([a]) = (a_1/a_0, ..., a_n/a_0)$, is a bijection.

Proof: If $\Phi([a]) = \Phi([b])$, then $a_i/a_0 = b_i/b_0$ for all i. Let $c = b_0/a_0 \in F^\times$. Then $a_i = cb_i$, which implies that $[a] = [b]$, so Φ is injective. Let for any $a = (a_1, ..., a_n) \in A^n(F)$, take $b = (1, a_1, ..., a_n) \in P^n(F) \setminus H$. Then $\Phi([b]) = a$, so that Φ is surjective. □

Hence Proposition 2.1 tells us that $P^n(F)$ is made up of $A^n(F)$ and $P^{n-1}(F)$.

2.2. **Polynomials and Hypersurfaces.**
Let $F[x_1, ..., x_n]$ be the ring of polynomials in n variables over the field F. Any $f \in F[x_1, ..., x_n]$ can be written as

$$f(x) = \sum_{(i_1,...,i_n)} a_{i_1 i_2 \cdots i_n} x_1^{i_1} x_1^{i_2} \cdots x_n^{i_n},$$

and the terms of the form $x_1^{i_i} \cdots x_n^{i_n}$ are called monomials. The sum $i_1 + ...i_n$ is called the total degree of the monomial and deg f will denote the maximum of the total degrees of monomials in $f(x)$. A polynomial whose monomials all have total degree l is called a homogeneous polynomial of degree l.

Let K be a field extension of F and $f \in F[x_1, ..., x_n]$. For $a \in A^n(K)$, we can consider the evaluation map

$$\varphi : A^n(K) \to K, \quad \varphi(a) = f(a) \text{ (substituting } a_i \text{ for } x_i).$$

Definition 2.3. The points a such that $f(a) = 0$ are called the *zeros* of f and the set

$$H_f(K) = \{a \in A^n(K) : f(a) = 0\}$$

is called the *hypersurface* defined by f.

In the case of f being a homogeneous polynomial of degree l, we have that $f(ca) = c^l f(a) = 0$ for all $c \in K^\times$. Hence we can similarly define a *projective hypersurface*

$$\overline{H}_f(K) = \{[a] \in P^n(K) : f(a) = 0\}.$$

For any given $f \in F[x_1, ..., x_n]$ and $y = (y_0, ..., y_n)$, define $\overline{f}(y) = y_0^{degf} f(y_1/y_0, ..., y_n/y_0)$. This defines a homogeneous polynomial of degree equal to f. This is called the *projective closure* of an affine hypersurface.

2.3. **Chevalley's Theorem.**
In this section the field F will be a finite field with q elements. The existence of solutions to any given equation is non-trivial in general. However, the following theorem by Claude Chevalley gives us the existence of non-trivial solutions to projective hypersurfaces over a finite field F when the number of variables in $F[x_1, ..., x_n]$ exceeds the degree of the polynomial.

Theorem 2.2. Let $f \in F[x_1, ..., x_n]$. Assume that $f(0, ..., 0) = 0$ and that deg $f < n$. Then f has more than one zero.

To prove this statement we will need a couple lemmas.

Lemma 2.3. If a polynomial $f \in F[x_1, ..., x_n]$ has degree less than q and vanishes on all of $A^n(F)$, then f is identically zero.

Proof: We proceed by induction on n. When $n = 1$ we have that a polynomial in one variable of degree less than q vanishes on all of F, and hence must be identically zero. Now assume that this is true for polynomials in $n - 1$ variables. Let $f(x_1, ..., x_n) \in F[x_1, ..., x_n]$. Then we may write f in terms of x_n as the following:

$$f(x_1, ..., x_n) = \sum_{i=0}^{q-1} g_i(x_1, ..., x_{n-1}) x_n^i.$$

For any $a \in A^{n-1}(F)$ and substituting a in g, we have that

$$f(a_1, ..., a_{n-1}, x_n) = \sum_{i=0}^{q-1} g_i(a_1, ..., a_{n-1}) x_n^i$$

is a polynomial in x_n which vanishes on F. Hence by the base case $g_i(a_1, ..., a_{n-1}) = 0$ for all i. By induction hypothesis, since a is arbitrary, g_i must be identically zero, and hence f. □

Definition 2.4. Let $f, g \in F[x_1, ..., x_n]$. We say f is equivalent to g, $f \sim g$ if $f(a) = g(a)$ for all $a \in A^n(F)$. A polynomial is called *reduced* if each variable has degree less than q.

Lemma 2.4. Every $f \in F[x_1, ..., x_n]$ is equivalent to a reduced polynomial.

Proof: Note that it is enough to show this for the case of a single variable since for a given monomial $x_1^{i_1} \cdots x_n^{i_n}$, we can reduce each variable individually and each will have degree less than q. Because $x^q - x = 0$ over F, we have that $x^q \sim x$. For arbitrary k, let j be minimal such that $x^k \sim x^j$. Now it must be the case. that $j < q$. For if not, then by the division algorithm there is an $a, b \in \mathbb{Z}$ such that $j = qa + b$ with $a > 0$ and $0 \leq b < q$. Then $x^k \sim x^j = x^{qa}x^b \sim x^a x^b = x^{a+b}$, and $a + b < j$, contradicting the fact that j was minimal. □

We can now prove Chevalley's Theorem:

Proof of Theorem 2.2: Let $f \in F[x_1, ..., x_n]$ be of degree d and suppose to the contrary that $\mathbf{0}$ is the only zero. Then the polynomial $1 - f^{q-1}$ has the property that $(1 - f^{q-1})(\mathbf{0}) = 1$ and zero elsewhere. Notice that the polynomial

$$(1 - x_1^{q-1})(1 - x_2^{q-1}) \cdots (1 - x_n^{q-1})$$

has the same property. By Lemma 2.4, $1 - f^{q-1}$ is equivalent to a reduced polynomial r, so the polynomial

$$r - (1 - x_1^{q-1}) \cdots (1 - x_n^{q-1})$$

vanishes on $A^n(F)$ and has degree $n(q-1)$ (since $\deg r < q$). By Lemma 2.3 we have that $r - (1 - x_1^{q-1}) \cdots (1 - x_n^{q-1})$ is identically zero. Hence $r = (1 - x_1^{q-1}) \cdots (1 - x_n^{q-1})$, implying that r has degree $n(q-1)$. Since r is the reduced form of f, we have that $\deg r \leq \deg f$, and so $n(q-1) \leq d(q-1)$. Thus $n \leq d = \deg f$, which is a contradiction. □

3. Trace and Norm over Finite Fields

We will use the fact that any finite extension $\mathbb{F}_p$ is Galois, for if E has p^n elements then E is the splitting field of the separable polynomial $x^{p^n} - x$ and splitting fields are unique up to isomorphism.

3.1. **Trace and Norm.**

Let E/F be a field extension.

Definition 3.1. The trace and norm of an element $\alpha \in E$ are defined to be the trace and determinant, respectively, of the endomorphism given by left multiplication

$$T : E \to E, \quad T(\beta) = \alpha\beta,$$
$$\mathrm{Tr}_{E/F}(\alpha) = \mathrm{Tr}(T), \quad N_{E/F}(\alpha) = \det(T).$$

It is a basic result in algebraic number theory that if E/K is a finite separable extension, then we may consider all F-embeddings $\sigma \in \mathrm{Hom}(E, \overline{F})$, where $\overline{F}$ is an algebraic closure of F and obtain the following:

Lemma 3.1. Let $\{\sigma_1, ..., \sigma_n\}$ be the F-embeddings of E into $\overline{F}$. Then

$$\mathrm{Tr}_{E/F}(\alpha) = \sum_{i=1}^{n} \sigma(\alpha), \quad N_{E/F}(\alpha) = \prod_{i=1}^{n} \sigma_1(\alpha).$$

We will mostly be considering The next lemma is also useful as it shows that the trace and norm are transitive.

Lemma 3.2. Let $F \subseteq E \subseteq K$ be a chain of fields and $\alpha \in K$. Then

$$\mathrm{Tr}_{K/F}(\alpha) = \mathrm{Tr}_{E/F}(\mathrm{Tr}_{K/E}(\alpha)), \quad N_{K/F}(\alpha) = N_{E/F}(N_{K/E}(\alpha)).$$

We will be primarily interested in the case where $F = \mathbb{F}_p$. Since any finite extension of $\mathbb{F}_p$ is Galois, these embeddings can be seen as the Galois conjugates of α for any $\alpha \in E$. It is a fact from finite field theory that $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F})$ is generated by the Frobenius endomorphism $\sigma : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$, $\sigma(\alpha) = \alpha^p$. More generally, for any finite field F of order $q = p^k$, we have that $\mathrm{Gal}(F_s/F)$ (where F_s is an extension of F of degree s) is cyclic of order s generated by σ^k. This gives us a way of writing an the trace and norm of any $\alpha \in F_s$ as

$$\mathrm{Tr}_{F_s/F}(\alpha) = \sum_{i=0}^{s-1} \alpha^{q^i}, \quad N_{F_s/F}(\alpha) = \prod_{i=0}^{s-1} \alpha^{q^i}.$$

For more on trace and norm of field extensions, one can refer to Jürgen Neukirch's *Algebraic Number Theory* [3].

4. Characters, Gauss Sums, and Jacobi Sums over Finite Fields

Characters play in an important role in our discussion on solutions of $x^n + y^n + z^n = 0$ over F in the case where n divides $q-1$. It turns out that over these finite fields the number of solutions to equations of the form $x^m = a$ can be written explicitly in terms of characters, which will be fruitful in our computations.

4.1. **Characters.**

Definition 4.1. A character of a finite abelian group G is a map $\chi : G \to \mathbb{C}^\times$ such that $\chi(ab) = \chi(a)\chi(b)$ for all $a, b \in G$.

For example, the character $\mathbf{1}$, $\mathbf{1}(a) = 1$ for all $a \in G$, is known as the trivial character. Since finite fields are finite abelian groups, we will be most interested in studying the case where $G = F^\times$, the multiplicative group of a finite field. A few observations that are immediate from the definition and the structure of finite fields are that $\chi(1) = 1$; if $|F| = q$, then $\chi(a)^{q-1} = \chi(a^{q-1}) = \chi(1) = 1$ (i.e. $\chi(a)$ is a $(q-1)st$ root of unity), and $\chi(a)^{-1} = \overline{\chi(a)}$, the complex conjugate of $\chi(a)$. One of the most useful basic results whose argument is used frequently is the following proposition:

Proposition 4.1. If χ is not trivial, then

$$\sum_{a \in F} \chi(a) = 0.$$

If χ is trivial, then this sum is $|F|$.

Proof: Since χ is not trivial, there is a $b \in F$ such that $\chi(b) \neq 1$. Let $S = \sum_{a \in F} \chi(a)$. Note that as ab varies through F as a does. Hence

$$\chi(b)S = \sum_{a \in F} \chi(ab) = S.$$

Hence $(\chi(b) - 1)S = 0$. Since $\chi(b) \neq 1$, we deduce that $S = 0$. □

By defining a multiplication of characters χ, λ of G to be $\chi\lambda(a) = \chi(a)\lambda(a)$, $\chi^{-1}(a) = \chi(a^{-1})$, then the characters of G form a group with identity element $\mathbf{1}$. In fact, if G is cyclic, then the characters form a cyclic group:

Theorem 4.2. If G is a cyclic group of order n, then the characters of G form a cyclic group of order n.

Proof: Let g be a generator of G. Then $g^n = 1$, which implies that $\chi(g)^n = \chi(g^n) = 1$ for all characters χ of G. As every element of G is a power of g, we have that all characters are nth roots of unity, which implies that the number of characters is at most n. Let $\chi(g^k) = e^{2\pi ki/n}$. Then χ is a character on G and $\chi(g^k) = \chi(g)^k$, so χ is completely determined by g. $e^{2\pi i/n}$ is a primitive nth root of unity, and $\chi(g^k) = \chi(g^l)$ implies $e^{2\pi ki/n} = e^{2\pi li/n}$ (or $e^{2\pi(k-l)i/n} = 1$), so that $k \equiv l \pmod{n}$. In particular, n is the smallest positive integer such that $\chi(g)^n = 1$ as $e^{2\pi mi/n} = 1$ if and only if $n|m$. Thus there are n distinct characters of G generated by $\chi(g)$. □

One immediately sees from this that for all $a \in G$ with $a \neq 1$, then there is a character χ such that $\chi(a) \neq 1$. In fact, letting g be a generator of G and $\lambda(g)$ being the the generator of the group of characters, we see that if $a = g^k \neq 1$ (so $n \nmid k$), then $\chi(a) = e^{2\pi ki/n} \neq 1$. This

observation also shows that for all $a \neq 1$:

$$\sum_{\chi} \chi(a) = 0,$$

where is the sum is taken over all characters of G, by using the same strategy as in Proposition 3.1 by multiplying the sum by the appropriate $\chi(a) \neq 1$ and using the fact that characters are a group.

Now we consider the case where $G = \mathbb{F}_p^\times$. As the multiplicative group of a finite field is cyclic and $\mathbb{F}_p^\times$ has $p-1$ elements, the character group of $\mathbb{F}_p^\times$ is a cyclic group of order $p-1$ by Theorem 3.2. It is useful in many situations to extend a character to all of $\mathbb{F}_p$. By setting $\mathbf{1}(0) = 1$ and $\chi(0) = 0$ for all non-trivial χ, we extend the homomorphism property as a function from $\mathbb{F}_p$ to $\mathbb{C}$. To relate the theory of characters to solutions of equations over $\mathbb{F}_p$, it is useful to first deal with solutions of monomials modulo p. Let $N(x^n = a)$ denote the number of solutions in $\mathbb{F}_p$. Observe that in order to have a character of $\mathbb{F}_p^\times$, we must require that it be a $(p-1)$st root of unity, so if $n|p-1$, we obtain the following lemma:

Lemma 4.3. If $n|p-1$, then $N(x^n = a) = \sum_\chi \chi(a)$, where the sum is taken over all characters χ of order dividing n.

Proof: By Theorem 4.2, the character group of $\mathbb{F}_p^\times$ is generated by some $\chi(g) = e^{2\pi i/p-1}$, where g is a generator of $\mathbb{F}_p^\times$. Since $n|p-1$, we can define a new character $\gamma(g) = (e^{2\pi i/p-1})^{\frac{p-1}{n}} = e^{2\pi i/n}$, which generates the nth roots of unity. Note that there are n distinct powers of γ since χ has order $p-1$. Hence there are n characters of order dividing n.
We now consider the case where $a = 0$. Then $x^n = 0 \pmod p$ has the unique solution $x = 0$, which implies that $N(x^n = 0) = 1$. Note that the trivial character is of order dividing n, and so the sum in the statement contains a 1. As all non-trivial characters send zero to zero, this gives us the claim.
Now suppose $x^n = a \pmod p$ is solvable. Then there are n unique solutions to this equation. Let x_0 be a particular solution. Since all characters in the sum have order dividing n, $\chi(a) = \chi(x_0^n) = \chi(x_0)^n = 1$ for all χ. Thus the sum is just n as well.
Now suppose $x^n = a \pmod p$ is not solvable. Then $N(x^n = a) = 0$. Letting g and γ be as above with $a = g^k$, and, since $x^n = a$ is not solvable, $k \nmid n$. Hence $\gamma(a) = \gamma(g)^k \neq 1$. Letting $S = \sum_\chi \chi(a)$ be the sum in the statement, we have that

$$\gamma(a)S = S \implies (\gamma(a) - 1)S = 0 \implies S = 0$$

since γ permutes the characters of $\mathbb{F}_p^\times$, which gives us the claim. □

4.2. **Gauss Sums.**
Gauss sums will be important to understanding the number of points on a projective hypersurfaces. In fact, we will be able to write the number of solutions of a hypersurface based off Jacobi sums, which for the most part can be computed using Gauss sums (which are easier to compute in general). To define the Gauss sum, let $\zeta = e^{2\pi i/p}$.

Definition 4.2. Let F be a finite field, χ a character on F, and $\alpha \in F$. Define the *Gauss sum* of χ to be

$$g_\alpha(\chi) = \sum_{a \in F} \chi(a)\zeta^{\mathrm{Tr}_{F/\mathbb{F}_p}(\alpha a)}.$$

Note that it is simple to compute $g_\alpha(\chi)$ when $\chi = \mathbf{1}$, the trivial character. If $\alpha = 0$, then $g_0(\chi) = q$ since $\chi(a) = 1$ for all $a \in F$ and $e^0 = 1$. If $\alpha \neq 0$, then
We will be more interested in the case where χ is not trivial. Notice that for such χ and $\alpha \neq 0$,

$$\chi(\alpha)g_\alpha(\chi) = \sum_{a\in F} \chi(\alpha a)\zeta^{\mathrm{Tr}_{F/\mathbb{F}_p}(\alpha a)} = g_1(\chi),$$

so we have the relation that $g_\alpha(\chi) = \chi(\alpha^{-1})g_1(\chi)$. If $\alpha = 0$, then the sum is 0 as $\chi(0) = 0$ for nontrivial χ. We will let $g(\chi) = g_1(\chi)$ throughout the rest of this paper for simplicity. Gauss sums can become quite difficult to compute as the character varies, but we always know its magnitude. Ireland and Rosen give the wonderful proof of the following lemma:

Lemma 4.4. Suppose $\chi \neq \mathbf{1}$ and $\alpha \neq 0$. Then $|g_\alpha(\chi)| = \sqrt{q}$.

Proof: Since $g_\alpha(\chi) = \chi(\alpha^{-1})g(\chi)$, it is enough to show that $|g(\chi)| = \sqrt{q}$. To show the equality, we will evaluate the sum

$$\sum_{a\in F} g_a(\chi)\overline{g_a(\chi)}.$$

By our above observations, we have for $a \in F^\times$: $g_a(\chi) = \chi(a^{-1})g(\chi)$, so

$$g_a(\chi)\overline{g_a(\chi)} = \chi(a^{-1})g(\chi)\chi(a)\overline{g(\chi)} = |g(\chi)|^2.$$

For $a = 0$ the Gauss sum is zero, so taking the sum over all a gives $(q-1)|g(\chi)|^2$.
Directly computing the sum, we see that

$$g_a(\chi)\overline{g_a(\chi)} = \sum_{s\in F} \chi(s)\zeta^{\mathrm{Tr}_{F/\mathbb{F}_p}(sa)} \sum_{t\in F^\times} \chi(t^{-1})\zeta^{\mathrm{Tr}_{F/\mathbb{F}_p}(ta)} = \sum_{s,t\in F^\times} \chi(st^{-1})\zeta^{\mathrm{Tr}_{F/\mathbb{F}_p}((s-t)a)}.$$

Let S denote the last sum above. Since Tr is an additive function, we can pull out the a and get

$$S = \sum_{s,t\in F^\times} \chi(st^{-1})(\zeta^{\mathrm{Tr}_{F/\mathbb{F}_p}(s-t)})^a.$$

Since $\mathrm{Tr} : F \to \mathbb{F}_p$, $\zeta^{\mathrm{Tr}_{F/\mathbb{F}_p}(s-t)}$ is just a power of ζ, and hence remains a p-th root of unity. Summing over a gives

$$\sum_{a\in F} S = \sum_{s,t\in F^\times} \chi(st^{-1}) \sum_{a\in F} (\zeta^{\mathrm{Tr}_{F/\mathbb{F}_p}(s-t)})^a.$$

If $s - t \neq 0$, then this inner sum is, or else it is $|F| = q$. In this case, $\chi(st^{-1}) = 1$, and so we just get q for all pairs $(s, t) \in F^\times \times F^\times$ such that $s = t$. Since t is completely determined by s, there are $q - 1$ ways this can happen, and so $\sum_{a\in F} g_a(\chi)\overline{g_a(\chi)} = (q-1)q$. Comparing both ways we evaluated the sum, we get that

$$(q-1)|g(\chi)|^2 = (q-1)q,$$

and hence $|g(\chi)| = \sqrt{q}$. □

4.3. **Jacobi Sums.**

At first sight, the Jacobi sum does not appear to give much information or intuition on its usefulness in computing the number of points. To deal with this, we motivate this definition with an example. Consider the equation

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

When $n|p-1$, we may ask for $N(x^n+y^n=1)$ using characters of order dividing n. Notice that we can look at the equation $a+b=1$ and ask for $N(x^n=a)$ and $N(y^n=b)$, giving us $N(x^n=a)N(y^n=b)$ possible solutions to the equation. Hence

$$N(x^n+y^n=1)=\sum_{a+b=1}N(x^n=a)N(y^n=b)$$

$$=\sum_{a+b=1}\Big(\sum_{\chi}\chi(a)\Big)\Big(\sum_{\lambda}\lambda(b)\Big)=\sum_{\chi,\lambda}\Big(\sum_{a+b=1}\chi(a)\lambda(b)\Big),$$

where the sum is over all characters χ,λ of order dividing n. This inner sum is what we will be studying and will be the *Jacobi sum*. It is more interesting to immediately generalize this notion to multiple characters.

Definition 4.3. Let $\chi_1,...,\chi_n$ be characters on a finite field F. The Jacobi sum is defined to be

$$J(\chi_1,...,\chi_n)=\sum_{\sum a_i=1}\chi_1(a_1)\cdots\chi_n(a_n).$$

We also define the sum that represents Fermat hypersurfaces, the focus of this paper, as:

$$\hat{J}(\chi_1,...,\chi_n)=\sum_{\sum a_i=0}\chi_1(a_1)\cdots\chi_n(a_n).$$

We first make some quick observations that allow us to compute or even simplify the Jacobi sum.

Proposition 4.5. (a) If $\chi_i=\mathbf{1}$ for all i, then $J(\chi_1,...,\chi_n)=\hat{J}(\chi_1,...,\chi_n)=q^{n-1}$.
(b) If at least one but not all $\chi_i=\mathbf{1}$, then $J(\chi_1,...,\chi_n)=\hat{J}(\chi_1,...,\chi_n)=0$.
(c) If $\chi_n\neq\mathbf{1}$, then

$$\hat{J}(\chi_1,...,\chi_n)=\begin{cases}0, & \text{if } \chi_1\cdots\chi_n\neq\mathbf{1}\\ \chi_n(-1)(q-1)J(\chi_1,...,\chi_{n-1}), & \text{otherwise}\end{cases}$$

Proof: (a) Note that there are q^{n-1} solutions to the equation $a_n=-a_1-...-a_{n-1}$ by varying $a_1,...,a_{n-1}\in F$. Since all χ_i are trivial, we are just adding 1 q^{n-1}-many times, and so $\hat{J}(\chi_1,...,\chi_n)=q^{n-1}$. We can do the same thing for $J(\chi_1,...,\chi_n)$ since the equation $a_n=1-a_1-...-a_{n-1}$ also has q^{n-1} solutions.
(b) Without loss of generality, we can assume that χ_1 is nontrivial and χ_n is trivial. Since we can write $a_n=-a_1-...-a_{n-1}$ as in (a) and $\chi_n(a_n)=1$ for all a_n, we can drop the constriction and get

$$\hat{J}(\chi_1,...,\chi_n)=\sum_{a_1,...,a_{n-1}}\chi_1(a_1)\cdots\chi_{n-1}(a_{n-1})=\Big(\sum_{a_1}\chi_1(a_1)\Big)\sum_{a_2,...,a_{n-1}}\chi_2(a_2)\cdots\chi_{n-1}(a_{n-1})=0$$

by Proposition 4.1. This works the same way for $J(\chi_1,...,\chi_n)$ as in (a).
(c) If $\chi_n\neq 1$, then $\chi_n(0)=0$, and so we can write

$$\hat{J}(\chi_1,...,\chi_n)=\sum_{a_n\neq 0}\Big(\sum_{a_1+...+a_{n-1}=-a_n}\chi_1(a_1)\cdots\chi_{n-1}(a_{n-1})\Big)\chi_n(a_n).$$

Since $a_n\neq 0$ in this sum, we can write $a_i=-a_nb_i$ for some b_i and all $i=1,...,n-1$. This inner sum then becomes

$$\sum_{b_1+...+b_{n-1}=1}\chi_1(-a_nb_1)\cdots\chi_{n-1}(-a_nb_{n-1})=\sum_{b_1+...+b_{n-1}=1}\chi_1\cdots\chi_{n-1}(-a_n)\chi_1(b_1)\cdots\chi_{n-1}(b_{n-1}).$$

We are thus left with

$$\hat{J}(\chi_1, ...\chi_n) = \chi_n(-1) \sum_{a_n \neq 0} \chi_1 \cdots \chi_n(a_n) J(\chi_1, ..., \chi_{n-1}).$$

By Proposition 4.1, this sum will be zero if $\chi_1 \cdots \chi_n$ is not trivial, and $\chi_n(-1)(q-1)J(\chi_1, ..., \chi_{n-1})$ if it is trivial, giving us the claim. □

This proposition makes computing the number of solutions easier. For example, consider the hypersurface defined by the polynomial $x^2 + y^2 = 1$ over $\mathbb{F}_p$ for any odd prime p (so $2|p-1$). The character of order 2 is the Legendre symbol $(\frac{\cdot}{p})$. Hence $N(x^2 = a) = 1 + (\frac{a}{p})$ Then

$$\begin{aligned} N(x^2 + y^2 = 1) &= \sum_{a+b=1} N(x^2 = a) N(y^2 = b) = \sum_{a+b=1} \Big(1 + \Big(\frac{a}{p}\Big) + \Big(\frac{b}{p}\Big) + \Big(\frac{a}{p}\Big)\Big(\frac{b}{p}\Big)\Big) \\ &= J(\mathbf{1}, \mathbf{1}) + J(\chi, \mathbf{1}) + J(\mathbf{1}, \chi) + J(\chi, \chi). \end{aligned}$$

By the proposition, the first term is p, the middle two terms are 0, so all that is left is to figure out what $J(\chi, \chi)$ is. In this case, $\chi = \chi^{-1}$, and we prove a more general result:

Proposition 4.6. $J(\chi, \chi^{-1}) = -\chi(-1)$.

Proof: By definition,

$$J(\chi, \chi^{-1}) = \sum_{a+b=1} \chi(a)\chi^{-1}(b).$$

From $a + b = 1$, we have $ab^{-1} = \frac{a}{1-a}$ where $a \neq 1$. Thus χ takes all values $\frac{a}{1-a}$ in F except for the value -1 (if $\frac{a}{1-a} = x$, then $a = \frac{x}{1+x}$ for $x \neq -1$), and hence

$$J(\chi, \chi^{-1}) = -\chi(-1).$$

□

This proposition gives us that $N(x^2 + y^2) = p - \chi(-1) = p - (\frac{-1}{p})$. Elementary number theory classifies this Legendre symbol for all odd primes p as

$$\Big(\frac{-1}{p}\Big) = \begin{cases} 1, & p \equiv 1 \pmod 4 \\ -1, & p \equiv 3 \pmod 4. \end{cases}$$

Thus $N(x^2 + y^2 = 1) = p - 1$ if $p \equiv 1 \pmod 4$ and $N(x^2 + y^2 = 1) = p + 1$ if $p \equiv 3 \pmod 4$. We now show the relation between Gauss sums and Jacobi sums.

Proposition 4.7. (a) Let $\chi_1, ..., \chi_n$ and $\chi_1 \cdots \chi_n$ be nontrivial characters. Then

$$g(\chi_1) \cdots g(\chi_n) = J(\chi_1, ..., \chi_n) g(\chi_1 \cdots \chi_n).$$

Proof: (a)

$$g(\chi_1) \cdots g(\chi_n) = \Big(\sum_{t_1} \chi_1(t_1)\zeta^{t_1}\Big) \cdots \Big(\sum_{t_n} \chi_n(t_n)\zeta^{t_n}\Big) = \sum_k \Big(\sum_{\sum t_i = k} \chi_1(t_1) \cdots \chi_n(t_n)\Big)\zeta^k.$$

If $k = 0$, then Proposition 4.5(c) implies that the inner sum is 0. When $k \neq 0$, substitution gives us that

$$\sum_{\sum t_i = k} \chi_1(t_1) \cdots \chi_n(t_n) = \chi_1\chi_2 \cdots \chi_n(k) J(\chi_1, ..., \chi_n).$$

Thus

$$g(\chi_1) \cdots g(\chi_n) = \sum_{k \neq 0} \chi_1\chi_2 \cdots \chi_n(k)\zeta^k J(\chi_1, ..., \chi_n) = J(\chi_1, ..., \chi_n) g(\chi_1 \cdots \chi_n). \quad \square$$

4.4. **The equation $y = a_1x_1^m + ... + a_nx_n^m$ and the Main Theorem.**

Theorem 4.8. Let F be a field with q elements. If $q \equiv 1 \pmod{m}$, then the number of points on hypersurface defined by the equation $a_0x_0^m + ... + a_nx_n^m = 0$ is

$$N = q^{n-1} + q^{n-2} + ... + 1 + (q-1)^{-1} \sum_{\chi_0,...,\chi_n} \chi_0(a_0^{-1}) \cdots \chi_n(a_n^{-1}) \hat{J}(\chi_0, ..., \chi_n),$$

where $\chi_i \neq \mathbf{1}$ and $\chi_i^m = \mathbf{1}$ (i.e. the nontrivial characters of order dividing m), and $\chi_0 \cdots \chi_n = \mathbf{1}$. In this case,

$$\frac{1}{q-1} \hat{J}(\chi_0, ..., \chi_n) = \frac{1}{q} g(\chi_0) \cdots g(\chi_n).$$

Proof: First observe that

$$N(a_0x_0^m + ... + a_nx_n^m = 0) = \sum_{\sum a_it_i = 0} N(x_0^m = t_0) \cdots N(x_n^m = t_n).$$

Since $m|q-1$, for each i,

$$N(x_i^m = t_i) = \sum_{\chi} \chi(t_i)$$

where the sum ranges over all characters of order dividing m. Hence

$$N(a_0x_0^m + ... + a_nx_n^m = 0) = \sum_{\chi_0,...,\chi_n} \sum_{\sum a_it_i = 0} \chi_0(t_0) \cdots \chi_n(t_n).$$

By the substitution $s_i = a_it_i$, we can reduce this to

$$\sum_{\chi_0,...,\chi_n} \hat{J}(\chi_0, ..., \chi_n).$$

From using the results in Proposition 4.5, we see that we can eliminate the summands where at least one, but not all, χ_i are trivial. We could also take all χ_i to be trivial to get q^n. Hence

$$N(a_0x_0^m + ... + a_nx_n^m = 0) = q^n + \sum_{\chi_0,...,\chi_n} \hat{J}(\chi_0, ..., \chi_n),$$

where the sum is over the characters given in the theorem. Note that these are points on affine A^{n+1} space. Hence if we want projective zeros, the number of zeros is given by

$$\frac{N(a_0x_0^m + ... + a_nx_n^m = 0) - 1}{q-1} = \frac{q^n - 1}{q-1} + (q-1)^{-1} \sum_{\chi_0,...,\chi_n} \hat{J}(\chi_0, ..., \chi_n)$$

and the first claim follows by geometric sums. The last claim follows from propositions 4.5(c) and 4.7. □

Note that in the case of Fermat hypersurfaces, $a_i = 1$ for all i. So to calculate the number of points on the hypersurface defined by $x_0^m + ... + x_n^m = 0$ is given by

$$N = q^{n-1} + q^{n-2} + ... + 1 + (q-1)^{-1} \sum_{\chi_0,...,\chi_n} J(\chi_0, ..., \chi_n).$$

Thus our problem boils down to being able to compute these Jacobi sums or Gauss sums.

5. Zeta Function on Projective Hypersurfaces

We now introduce the zeta function for projective hypersurfaces.

5.1. **Zeta Function.**

Let F be a finite field of order q, and let F_s/F be an extension of degree s (containing q^s elements). Fix a homogeneous polynomial $f \in F[x_0, ..., x_n]$ and define N_s to be the number of points in $\overline{H}_f(F_s)$. Note that since any two finite fields of the same order are isomorphic, it follows that N_s is independent on the choice of F_s, hence N_s only depends on s. If we consider the power series

$$\sum_{s=1}^{\infty} N_s t^s,$$

then we may regard it as an analytic function with radius convergence q^{-n} (since we have $N_s \leq \frac{q^{s(n+1)}-1}{q^s-1} \leq (n+1)q^{sn}$), or simply as formal power series.

Definition 5.1. The zeta function of the hypersurface defined by $f \in F[x_0, ..., x_n]$ is given by

$$Z_f(t) = \exp\Big(\sum_{s=1}^{\infty} \frac{N_s t^s}{s}\Big).$$

One of the most interesting questions to ask about the zeta function of a hypersurface is whether it is rational, and if so, in what cases. First observe that $Z_f(0) = e^0 = 1$. If the zeta function were rational with $Z_f(t) = \frac{P(t)}{Q(t)}$ for some polynomials P and Q, then $P(0) = Q(0) = 1$, so we may assume that the constant term of P and Q are both 1. By scaling, we can thus write

$$Z_f(t) = \frac{\prod_{i=1}^{n}(1 - z_i t)}{\prod_{j=1}^{m}(1 - w_j t)}, \quad z_i, w_j \in \mathbb{C}.$$

Writing the zeta function in this way allows us to prove the following important theorem:

Theorem 5.1. $Z_f(t)$ is rational if and only if there are z_i, w_j in $\mathbb{C}$ such that

$$N_s = \sum_j w_j^s - \sum_i z_i^s.$$

Proof: If $Z_f(t)$ is rational, then we can write

$$Z_f(t) = \frac{\prod_{i=1}^{n}(1 - z_i t)}{\prod_{j=1}^{m}(1 - w_j t)}.$$

Then

$$\log(Z_f(t)) = \sum_{i=1}^{n} \log(1 - z_i t) - \sum_{i=1}^{m} \log(1 - w_j t).$$

By taking the derivative of both sides,

$$\frac{Z_f'(t)}{Z_f(t)} = \sum_{i=1}^{n} \frac{-z_i}{1 - z_i t} - \sum_{i=1}^{m} \frac{-w_j}{1 - w_j t}.$$

Using geometric series, we may write this is

$$\sum_{i=1}^{n} \Big(\sum_{s=0}^{\infty} -z_i^{s+1} t^s\Big) - \sum_{j=1}^{m} \Big(\sum_{s=0}^{\infty} -w_j^{s+1} t^s\Big).$$

Multiplying by t on both sides of our equation thus gives

$$t\frac{Z_f'(t)}{Z_f(t)} = \sum_{s=1}^{\infty}\Big(\sum_{j=1}^{m} w_j^s - \sum_{i=1}^{n} z_i^s\Big)t^s.$$

On the other hand, by definition,

$$Z_f(t) = \exp\Big(\sum_{s=1}^{\infty}\frac{N_s t^s}{s}\Big).$$

By taking log and the derivative, we also get that

$$t\frac{Z_f'(t)}{Z_f(t)} = \sum_{s=1}^{\infty} N_s t^s.$$

Thus by looking at the coefficients, we see that

$$N_s = \sum_{j=1}^{m} w_j^s - \sum_{i=1}^{n} z_i^s.$$

Conversely, suppose such z_i, w_j in $\mathbb{C}$ exist. Then we can write

$$Z_f(t) = \exp\Big(\sum_{s=1}^{\infty}\frac{(\sum w_j^s - \sum z_i^s)t^s}{s}\Big)$$

$$= \exp\Big(\Big(\sum_{j=1}^{m}\Big(\sum_{s=1}^{\infty}\frac{(w_j t)^s}{s}\Big) - \sum_{i=1}^{n}\Big(\sum_{s=1}^{\infty}\frac{(z_i t)^s}{s}\Big)\Big)\Big).$$

Because of the identity

$$-\log(1-w_j t) = \sum_{s=1}^{\infty}\frac{(w_j t)^s}{s}$$

for all j, and similarly for $z_i's$,

$$Z_f(t) = \exp\Big(\sum_{i=1}^{n}\log(1-z_i t) - \sum_{j=1}^{m}\log(1-w_j t)\Big) = \frac{\prod_{i=1}^{n}(1-z_i t)}{\prod_{j=1}^{m}(1-w_j t)}.$$

So $Z_f(t)$ is rational. □

We now want to show that the zeta function has integral coefficients. To do this, we require the notion of a prime divisor. Let $V \subseteq A^n(\overline{F})$ be an algebraic set and $\alpha = (a_1, ..., a_n) \in V$. Let F_d be the smallest extension of F that contains all a_i, we say that α is of degree d. Then $\alpha^q = (a_1^q, ..., a_n^q)$ is also in V as F is fixed by Frobenius. Hence $\alpha, \alpha^q, ..., \alpha^{q^{d-1}}$ are all distinct points in V, for if $\alpha^{q^i} = \alpha^{q^j}$ for some $1 \le i < j < d$, then $\alpha^{q^{j-i}} = 1$, and so $\alpha \in F_{j-i}$ and $0 < j - i < d$, which contradicts the minimality of d.

Definition 5.2. We call the set $\mathfrak{p} = \{\alpha, \alpha^q, ..., \alpha^{q^{d-1}}\}$ a prime divisor on V.

Lemma 5.2. $N_s = \sum_{d|s} d \cdot \#(\text{prime divisors of degree } d)$.

Proof: For any $\alpha \in V$, we can find a d such that $\alpha \in F_d$, and so the prime divisors partition V. From field theory, we know that $\alpha \in F_d$ for some $d|s$, as $F_d \subseteq F_s$ if and only if $d|s$. There are d elements in every prime divisor of degree d, and the equality follows. □

Proposition 5.3. $Z_V(t) = \prod_{\mathfrak{p}} \frac{1}{1-t^{\deg \mathfrak{p}}}$.

Proof: Let k_n be the number of prime divisors of degree n. Then

$$\prod_{\mathfrak{p}} \frac{1}{1-t^{\deg \mathfrak{p}}} = \prod_{n=1}^{\infty} \Big(\frac{1}{1-t^n}\Big)^{k_n}.$$

Taking the logarithmic derivative would give us

$$\frac{Z_V'(t)}{Z_V(t)} = \sum_{n=1}^{\infty} \frac{k_n n t^{n-1}}{1-t^n},$$

and so

$$t\frac{Z_V'(t)}{Z_V(t)} = \sum_{n=1}^{\infty} \frac{k_n n t^n}{1-t^n} = \sum_{n=1}^{\infty} k_n n \Big(\sum_{m=0}^{\infty} t^{mn}\Big).$$

The coefficient of t^s after dividing by t is

$$\sum_{s=1}^{\infty} \Big(\sum_{d|s} d k_d\Big) t^{s-1} = \sum_{s=1}^{\infty} N_s t^{s-1}$$

by Lemma 5.2. By integrating, we get

$$\log Z_V(t) = \sum_{s=1}^{\infty} \frac{N_s}{s} t^s,$$

and so

$$\prod_{\mathfrak{p}} \frac{1}{1-t^{\deg \mathfrak{p}}} = Z_V(t) = \exp\Big(\sum_{s=1}^{\infty} \frac{N_s}{s} t^s\Big).$$

□

6. The Weil Conjectures

All of the results we have seen are a part of much greater phenomena: the Weil Conjectures. Let F be a finite field of order q and $f \in F[x_0, x_1, ..., x_n]$ is homogenous of degree d. Assume that f is non-singular, i.e. that all partial derivatives of f share no common projective zeros in any algebraic extension of F (in algebraic geometry, we can work with a smooth projective variety). Then for the hypersurface defined by $f = 0$, B. Dwork and P. Deligne proved the following conjectures:

(1) (Rationality) There is a polynomial P such that

$$Z_f(t) = \frac{P(t)^{(-1)^n}}{(1-t)(1-qt)\cdots(1-q^{n-1}t)}.$$

(2) We can factor $P(t) = (1-z_1 t)\cdots(1-z_m t)$ and the map $z \to \frac{q^{n-1}}{a}$ is a bijection of the reciprocal roots z_i.

(3) (Riemann Hypothesis) $|z_i| = q^{(n-1)/2}$.

(4) $\deg P(t) = d^{-1}[(d-1)^{n+1} + (-1)^{n+1}(d-1)]$.

These proofs of these conjectures are far beyond the scope of this paper; one would need knowledge of Etalé cohomology. A good reference is Robin Hartshorne's *Algebraic Geometry* [1].

7. Hasse-Davenport Relation

The Hasse-Davenport relation will be one of the main tools in computing the zeta function as it allows us to compute Gauss sums in extensions of F based solely on characters of F. Let F_s/F be an extension of degree s. Let χ be a character of F and $\chi' = \chi \circ N_{F_s/F}$. Notice that χ' is a character as both the norm function and χ are multiplicative.

Theorem 7.1. $-g(\chi') = (-g(\chi))^s$.

To prove this, we will need a few observations and a lemma. The Gauss sum of a character χ over F is $g(\chi) = \sum_{a\in F} \chi(a)\zeta^{\mathrm{Tr}_{F/\mathbb{F}_p}(a)}$. To write the Gauss sum of a character χ' in F_s, we may use the above observation that $\chi' = \chi \circ N_{F_s/F}$. By transitivity of the trace given in section 3, we have that $\mathrm{Tr}_{F_s/\mathbb{F}_p} = \mathrm{Tr}_{F/\mathbb{F}_p} \circ \mathrm{Tr}_{F_s/F}$. Hence we can already see the relationship given by the theorem. Also note that $\zeta^{a+b} = \zeta^a\zeta^b$. We can then create a function as follows: for monic $f = t^n - a_{n-1}t^{n-1} + ... + (-1)^n a_0$, define

$$\mathscr{F}(f) = \chi(a_0)\zeta^{a_{n-1}}.$$

Notice that if $g = t^m - b_{m_1}t^{m-1} + ... + (-1)^m b_0$, then $fg = t^{m+n} - (a_{n-1} + b_{m-1})t^{m+n-1} + ... + (-1)^{m+n}a_0b_0$, and so

$$\mathscr{F}(fg) = \chi(a_0b_0)\zeta^{a_{n-1}+b_{m-1}} = \chi(a_0)\zeta^{a_{n-1}}\chi(b_0)\zeta^{b_{m-1}} = \mathscr{F}(f)\mathscr{F}(g),$$

i.e. $\mathscr{F}$ is multiplicative. From the basic properties of trace and norm and field theory, we automatically get the following lemma:

Lemma 7.2. Let $m_{\alpha,F}(t)$ be the irreducible polynomial of $\alpha \in F_s$ over F. Then

$$\mathscr{F}(m_{\alpha,F})^{s/d} = \chi'(\alpha)\zeta^{\mathrm{Tr}_{F_s/\mathbb{F}_p}(\alpha)}.$$

Proof of Theorem 6.1: First observe the relation

$$\sum_{f\in F[x]: f \text{ is monic}} \mathscr{F}(f)t^{\deg f} = \prod_{f\in F[x]: f \text{ is monic and irreducible}} (1 - \mathscr{F}(f)t^{\deg f})^{-1}.$$

To see this, expand the terms on the right into a geometric sum. Since $F[x]$ is a unique factorization domain, any monic polynomial can be written uniquely as a product of monic irreducible polynomials. Hence every monic polynomial will appear as a product of these geometric sums, and this only happens once.
we now partition the sum by degrees:

$$\sum_{f\in F[x]: f \text{ is monic}} \mathscr{F}(f)t^{\deg f} = \sum_{s=0}^{\infty} \Big(\sum_{\deg f = s} \mathscr{F}(f) \Big) t^s.$$

When $s = 0$, the only monic polynomial is $f = 1$, and so we need $\mathscr{F}(1) = 1$ for the above equality to hold.
When $s = 1$, the irreducible polynomials of degree 1 are of the form $x - a$ for $a \in F$. Hence

$$\sum_{\deg f = 1} \mathscr{F}(f) = \sum_{a\in F} \mathscr{F}(x-a) = \sum_{a\in F} \chi(a)\zeta^{\mathrm{Tr}_{F/\mathbb{F}_p}(a)} = g(\chi)$$

For $s \geq 2$, notice that if we take an arbitrary monic polynomial $f = x^s - a_{s-1}x^{s-1} + ... + a_0$, then $\mathscr{F}(f)$ will take all possible values of F for a_{s-1} and a_0 while letting the other coefficients vary. Thus

$$\sum_{\deg\ f=s} \mathscr{F}(f) = \Big(\sum_{a_{s-1}\in F} \chi(a_{s-1}) \Big) \cdots = 0.$$

This implies that

$$\prod_{f\in F[x]:f \text{ is monic and irreducible}} (1 - \mathscr{F}(f)t^{\deg\ f})^{-1} = 1 + g(\chi)t.$$

Taking the logarithmic derivative and multiplying by a factor of t gives

$$\sum_{f\in F[x]:f \text{ is monic and irreducible}} \frac{\mathscr{F}(f)\deg\ f t^{\deg\ f}}{1 - \mathscr{F}(f)t^{\deg\ f}} = \frac{g(\chi)t}{1 + g(\chi)t}.$$

Writing both sides in a geometric series gives:

$$\sum_{f} \Big(\sum_{k=1}^{\infty} \mathscr{F}(f)\deg\ f^k t^k \Big) = \sum_{s=1}^{\infty} (-1)^{s-1} g(\chi)^s t^s.$$

Looking at the coefficient of t^s on each side gives

$$(-1)^{s-1} g(\chi)^s = \sum_{\deg\ f | s} (\deg\ f) \mathscr{F}(f)^{s/\deg\ f})$$

Note that by Lemma 6.2 and taking every root of each polynomial, it follows that the right side is $g(\chi')$, which establishes the theorem. □

8. The Number of Solutions to $x^n + y^n + z^n = 0$

Let $\mathscr{H}_n$ denote the (projective) hypersurface defined by the equation $x^n + y^n + z^n = 0$ over the finite field F.

8.1. **The case $n = 1$.**
The case where $n = 1$ is simple. For the equation $x+y+z = 0$, we can simply write $z = -x-y$ and vary all $x, y \in F$. So if $|F| = q$, then there are q^2 solutions. More generally, for any Fermat hypersurface $x_1 + ... + x_m = 0$ with $m > 1$, we could write $x_m = -x_1 - ... - x_{m-1}$ to get that there are q^{m-1} solutions.

8.2. **The case $n = 2$.**
For this case we generalize to $x_1^n + ... + x_m^n = 0$ for m even. Then by Theorem 4.9, the number of points over F is given by

$$q^{n-2} + q^{n-1} + ... + q + 1 + (q-1)^{-1} \sum_{\chi_1,...,\chi_m} \hat{J}(\chi_1, ..., \chi_m)$$

where χ_i are the nontrivial characters of order 2 such that $\chi_1 \cdots \chi_m = \mathbf{1}$. This only holds when every character is the character of order 2, call it χ. Then

$$N_1 = q^{n-2} + q^{n-1} + ... + q + 1 + \chi(-1)\frac{1}{q} g(\chi)^m.$$

But $g(\chi)^2 = \chi(-1)q$, and hence

$$N_1 = q^{n-2} + q^{n-1} + ... + q + 1 + \chi(-1)^{\frac{m}{2}+1} q^{m/2-1}.$$

We focus on the case where -1 is a square or $\frac{m}{2} + 1$ is even. Then by the Hasse-Davenport relation,

$$N_s = q^{s(n-2)} + ... + q^s + 1 + q^{s(\frac{m}{2}-1)}.$$

Hence

$$Z(t) = \exp(\sum_{s=1}^{\infty} \frac{N_s t^s}{s}) = \exp\Big(\sum_{s=1}^{\infty} \frac{(q^{n-2}t)^s}{s} + ... + \frac{(qt)^s}{s} + \frac{t^s}{s} + \frac{(q^{m/2-1}t)^s}{s}\Big)$$

$$= (1 - q^{n-2}t)^{-1} \cdots (1 - qt)^{-1}(1 - t)^{-1}(1 - q^{m/2-1}t)^{-1}.$$

In the other case, we can see that $\chi_s(-1) = 1$ for the even extensions s and $\chi_s(-1) = -1$ in the odd degree extensions. Hence

$$Z(t) = (1 - q^{n-2}t)^{-1} \cdots (1 - qt)^{-1}(1 - t)^{-1}(1 + q^{m/2-1}t)^{-1}.$$

In the case of $x^2 + y^2 + z^2 = 0$, we can see from the proof of the main theorem that $N(x^2 + y^2 + z^2 = 0) = q + 1$ since there is no way to take an odd product of nontrivial characters of order 2 to obtain the trivial character. This also shows that for general for odd $m > 2$, we obtain $q^{m-2} + q^{m-1} + ... + q + 1$ solutions.

8.3. **The case $n = 3$.**
Let χ be a character of order 3. By Theorem 4.9,

$$N_1 = q + 1 + \frac{1}{q} g(\chi)^3 + \frac{1}{q} g(\chi^2)^3.$$

Let $\pi = J(\chi, \chi)$. One can inductively use the relation in Proposition 4.7(a) with all $\chi_i = \chi$ to deduce the following lemma:

Lemma 8.1. $g(\chi)^3 = q\pi$.

This lemma implies that $N_1 = q + 1 + \pi + \overline{\pi}$. By the Hasse-Davenport relation, we can also extend this to all extensions F_s as:

$$N_s = q^s + 1 - (-\pi)^s - (-\overline{\pi})^s.$$

Then

$$Z(t) = \exp\Big(\sum_{s=1}^{\infty} \frac{N_s}{s} t^s\Big) = \exp\Big(\sum_{s=1}^{\infty} \frac{q^s}{s} t^s\Big) \exp\Big(\sum_{s=1}^{\infty} \frac{t^s}{s}\Big) \exp\Big(-\sum_{s=1}^{\infty} \frac{(-\pi)^s}{s} t^s\Big) \exp\Big(-\sum_{s=1}^{\infty} \frac{(-\overline{\pi})^s}{s} t^s\Big)$$
$$= \frac{(1+\pi t)(1+\overline{\pi} t)}{(1-qt)(1-t)}.$$

8.4. **The case of $n > 3$.**
It is less obvious on how to proceed when $n > 3$. We can still use the main theorem to deduce that the number of points over F is given by

$$q + 1 + \sum_{\chi_1, \ldots, \chi_m} \hat{J}(\chi_1, ..., \chi_m)$$

where these χ_i are nontrivial characters of order n over F that satisfy $\chi_1 \cdots \chi_m = \mathbf{1}$. However, unlike the previous cases, there is no real way of knowing what the characters over arbitrary F look like. There also is not an obvious relation that simplifies the Gauss sums as in the $n = 3$ case.

It should be emphasized again here that these results come from the fact that $n|q-1$ so that we can define characters over F. If this relation does not hold, then this is either of no use, or we need a way to reduce the problem to something that we can apply the theory to.

References

[1] Robin Hartshorne. *Algebraic geometry*, volume 52. Springer, 1977.
[2] Kenneth Ireland and Michael Rosen. *A Classical Introduction to Modern Number Theory*. Springer Science and Business Media Inc., 1990.
[3] Jürgen Neukirch. *Algebraic Number Theory*, volume 322. Springer Science and Business Media Inc., 1999.