Abstract

We work over finite fields and their extensions. We determine the cardinality of the solution set of Fermat hypersurfaces. We calculate this cardinality in different ways: using character theory, namely Gauss- and Jacobi sums, and with projective- and algebraic geometry. We consider several special cases of Fermat hypersurfaces before giving a procedure for treating the general case. Based on these results, we prove the law of quadratic reciprocity and the Hasse-davenport relation. Finally we prove the rationality of Weil's generating function for the cardinality of the solution set of a general Fermat hypersurface.

Dansk resume

Vi arbejder over endelige legemer og deres udvidelser. Vi bestemmer kardinaliteten af løsningsmængden til Fermat hyperflader. Vi beregner denne kardinalitet på flere måder: ved brug af multiplikative karakterer, nærmere bestemt Gauss- og Jacobi summer, og ved brug af projektiv- og algebraisk geometri. Vi betragter flere specialtilfælde af Fermat hyperflader og giver en metode til behandling af den generaliserede Fermat hyperflade. På dette grundlag beviser vi loven om kvadratisk reciprocitet og Hasse-Davenport relationen. Til sidst beviser vi rationaliteten af Weils genererende funktion for kardinaliteten af løsningsmængden til en generel Fermat hyperflade.

Contents

Introduction

A familiar problem in maths is the study of integer solutions to the Fermat equation

$$a^n + b^n = c^n.$$

This thesis aims to generalize this type of equation and study the associated solution sets. We will treat equations on the form

$$a_1x_1^{m_1} + a_2x_2^{m_2} + ... + a_nx_n^{m_n} = b$$

$m_i \in \mathbb{N},\ i = 1, ...n$ and $a_i, x_i \in \mathbb{F},\ i = 1, ..., n$ where $\mathbb{F}$ is a finite field. We will typically restrict ourselves to the case where $\mathbb{F} = \mathbb{F}_p$ for p an odd prime, but later on we will look at solution sets in general field extensions.
The type of equation above is what we call a Fermat hypersurface. Denoting by $N_n(b)$ the cardinality of the solution set, i.e.

$$N_n(b) = \#\{a_1x_1^{m_1} + a_2x_2^{m_2} + ... + a_nx_n^{m_n} = b|(x_1, ..., x_n) \in \mathbb{F}_p^n\}$$

our goal here is to find different methods to determine this number. It turns out that this can be done in many different ways, for instance using character theory or geometry. Depending on which method we use, we can derive other results in the process, for instance the law of quadratic reciprocity.
In the last part of the thesis we will show a big result of Weil's, namely that we can associate the cardinality of a solution set corresponding to a field extension of any degree with a generating series which becomes a rational function.

The primary sources used for this thesis are Michael Rosen and Kenneth Ireland's *A Classical Introduction to Modern Number Theory* and André Weil's article *Numbers of Solutions of Equations in Finite Fields*; please see the references for details.

The thesis presupposes basic knowledge of algebra, and some algebraic number theory and -geometry, but most necessary results will be stated within.

Gauss and Jacobi sums

In this chapter we will cover some basic theory involving multiplicative characters, a particular type of map with useful properties. Particularly we will study various kinds of sums over multiplicative characters, results which we will use extensively later on when we start working on problems from number theory. These will be what we refer to as Gauss- and Jacobi sums. When not explicitly stated, any characters we work with are assumed to be multiplicative.
In the following we work over finite fields of the type $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ where p is an odd prime.

2.1 Multiplicative characters

A multiplicative character is a map from the multiplicative group $\mathbb{F}_p^*$ belonging to our field $\mathbb{F}_p$ into the non-zero complex numbers. Initially we work only with $\mathbb{F}_p^*$, but later on it will be useful to extend our maps to the whole field. More specifically we have:

Definition 2.1.1. *Let $\chi : \mathbb{F}_p^* \to \mathbb{C}\backslash\{0\}$. Then χ is a multiplicative character if it satisfies $\chi(ab) = \chi(a)\chi(b)$ for all $a, b \in \mathbb{F}_p^*$.*

Some examples of multiplicative characters are the Legendre symbol given by $\chi(a) = \left(\frac{a}{p}\right)$, and the trivial character ε, defined by $\varepsilon(a) = 1$ for all a in $\mathbb{F}_p^*$. We can also extend multiplicative characters to all of $\mathbb{F}_p$ by putting $\chi(0) = 0,\ \chi \neq \varepsilon$, and $\varepsilon(0) = 1$.

It is useful to to get an overview of the many properties of characters. Below we state and prove some useful results that lead up to larger theorems.

Proposition 2.1.2. *Let χ be a multiplicative character on $\mathbb{F}_p$ and let $a \in \mathbb{F}_p^*$. Then χ has the following properties:*
a) $\chi(1) = 1$;
b) $\chi(a)$ is a $(p-1)$st root of unity;
c) $\chi(a^{-1}) = \chi(a)^{-1} = \overline{\chi(a)}$.

Proof. a) First note that by definition $\chi(1) \neq 0$. We have that $\chi(1) = \chi(1 \cdot 1) = \chi(1)\chi(1)$, so $\chi(1) = 1$.
b) Since $a \in \mathbb{F}_p^*$, $a^{p-1} = 1$. This implies that $1 = \chi(1) = \chi(a^{p-1}) = \chi(a)^{p-1}$, i.e. χ is a $(p-1)$st root of unity.
c) We have that $1 = \chi(1) = \chi(a^{-1}a) = \chi(a^{-1})\chi(a)$, hence $\chi(a^{-1}) = \chi(a)^{-1}$. *b)* gives that $\chi(a)$ has absolute value one, and since $\chi(a)$ is a complex number, this implies that

$\chi(a)^{-1} = \overline{\chi(a)}$.

□

Proposition 2.1.3. *If χ is a multiplicative character, $\chi \neq \varepsilon$, then $\sum_{t\in\mathbb{F}_p} \chi(t) = 0$. If $\chi = \varepsilon$, then $\sum_{t\in\mathbb{F}_p} \varepsilon(t) = p$.*

Proof. It follows immediately that $\sum_{t\in\mathbb{F}_p} \varepsilon(t) = p$ by definition of ε and the fact that $\mathbb{F}_p$ has p elements. Assume $\chi \neq \varepsilon$. Then by definition, there exists an $a \in \mathbb{F}_p^*$ such that $\chi(a) \neq 1$. Let $T = \sum_{t\in\mathbb{F}_p} \chi(t)$. Recall that we defined $\chi(0) = 0$ so we can disregard this term and then we have a sum over elements of $\mathbb{F}_p^*$, which is a group. Then for a fixed non-zero a, at will also run through all the elements of $\mathbb{F}_p$ as t runs through these. Then we have

$$\chi(a)T = \sum_{t\in\mathbb{F}_p} \chi(a)\chi(t) = \sum_{t\in\mathbb{F}_p} \chi(at) = T.$$

Since we have $\chi(a) \neq 1$, it follows that $T = 0$. □

The characters on $\mathbb{F}_p$ form an abelian group with pointwise multiplication as operation so that:

a) $\chi\lambda(a) = \chi(a)\lambda(a)$ for all a in $\mathbb{F}_p^*$;

b) the neutral element is the trivial character ε;

c) the inverse, χ^{-1}, pertaining to a character χ, is the map that for all a in $\mathbb{F}_p^*$ maps to $\chi(a)^{-1} = \overline{\chi(a)}$.
By this we have the following result:

Proposition 2.1.4. *The group of characters is cyclic of order $p - 1$. Furthermore, if $a \neq 1 \in \mathbb{F}_p^*$, there exists a character χ such that $\chi(a) \neq 1$.*

Proof. We use that the characters form a group and the well-known fact that $\mathbb{F}_p^*$ is cyclic. Now let g be a generator for $\mathbb{F}_p^*$, so that every element $a \in \mathbb{F}_p^*$ can be expressed as a power of g. If $a = g^l$, then for any character χ it holds that $\chi(a) = \chi(g^l) = \chi(g)^l$. This shows that a character is completely determined by its value on the generator. We have shown previously that $\chi(g)$ is a $(p-1)$st root of unity, of which there are precisely $p - 1$. Hence the order of the character group can at most be $p - 1$.
Let $\lambda : \mathbb{F}_p^* \to \mathbb{C}\backslash\{0\}$ be defined by $\lambda(g^l) = e^{\frac{2\pi il}{p-1}}$. Then λ is well-defined and is a character on $\mathbb{F}_p^*$. Let n be the order of λ, i.e. the smallest integer such that $\lambda^n = \varepsilon$. Now we show that $n = p - 1$. We have that $\lambda^n(g) = \varepsilon(g) = 1$, but we also have that $\lambda^n(g) = \lambda(g)^n = e^{\frac{2\pi in}{p-1}}$, hence $p - 1|n$ (using the fundamental fact that $e^{2\pi i} = 1$ and $e^{2\pi i\frac{a}{b}} \neq 1$ if $\frac{a}{b} \notin \mathbb{Z}$).
Since $\lambda^{p-1}(a) = \lambda(a)^{p-1} = \lambda(a^{p-1}) = \lambda(1) = 1$, we have $\lambda^{p-1} = \varepsilon$.
As $\varepsilon, \lambda, \lambda^2, ..., \lambda^{p-1}$ are all distinct, and since we have shown that the number of characters can at most be $p - 1$, this gives that there are precisely $p - 1$ characters. It also shows that the character group is cyclic and that λ is a generator for this group.
Lastly, we show that if $p - 1 \not| l$, then for $a \in \mathbb{F}_p^*$, $a \neq 1$, and $a = g^l$, we have that

$\lambda(a) \neq 1$. This follows by calculation: $\lambda(a) = \lambda(g^l) = \lambda(g)^l = e^{\frac{2\pi i l}{p-1}} \neq 1$ by our assumption on l. □

This result also gives the following corollary abut character sums:

Corollary 2.1.4.1. *For $a \neq 1$, $a \in \mathbb{F}_p^*$, we have that*

$$\sum_{all\ characters\ \chi} \chi(a) = 0.$$

Proof. Denote by S the sum

$$S = \sum_{all\ characters\ \chi} \chi(a).$$

By the previous proposition, this sum is finite and there exists a character λ such that $\lambda(a) \neq 1$. Then we have that

$$\lambda(a)S = \sum_{all\ characters\ \chi} \lambda(a)\chi(a) = \sum_{all\ characters\ \chi} \lambda\chi(a) = S.$$

Since the characters form a group, then for a fixed λ, $\lambda\chi$ runs over all characters as χ does. Since $\lambda(a) \neq 1$, we must have $S = 0$. □

Now we start applying character theory to the study of equations and enumerating their solutions. We start by considering the special case $x^n = a$:

Proposition 2.1.5. *Let $a \in \mathbb{F}_p^*$ and $n|p-1$. If the equation $x^n = a$, $n \in \mathbb{N}$, has no solutions, then there exists a character χ such that*

$$\begin{aligned} &a) \quad \chi^n = \varepsilon; \\ &b) \quad \chi(a) \neq 1. \end{aligned}$$

Proof. Let g be a generator for $\mathbb{F}_p^*$ and let λ be the character as defined in the proof of proposition 2.1.4, i.e. $\lambda(a) = \lambda(g^l) = e^{\frac{2\pi i l}{p-1}}$ where g is a generator. Let $\chi = \lambda^{\frac{p-1}{n}}$. Then we have that

$$\chi(g) = \lambda^{\frac{p-1}{n}}(g) = \lambda(g)^{\frac{p-1}{n}} = e^{\frac{2\pi i \frac{p-1}{n}}{p-1}} = e^{\frac{2\pi i (p-1)}{n(p-1)}} = e^{\frac{2\pi i}{n}}.$$

Since g is a generator, $a = g^l$ for some l. The assumption that $x^n = a$ has no solutions implies that n cannot divide l, as we would have $x = g^{\frac{l}{n}}$. Then we have that

$$\chi(a) = \chi(g^l) = \chi(g)^l = e^{\frac{2\pi i l}{n}} \neq 1$$

which gives b). □

Let a be an element of $\mathbb{F}_p$. Then we consider the equation $x^n = a$ and let $N(x^n = a)$ denote the number of solutions. The following proposition gives a way of determining this number:

Proposition 2.1.6. *Let n be a divisor of $p-1$. Then it holds that*

$$N(x^n = a) = \sum_{\chi^n = \varepsilon} \chi(a)$$

where we sum over all characters χ of order dividing n.

Proof. We proceed by first proving the following small lemma:

Lemma 2.1.7. *There are precisely n characters of order dividing n.*

Proof. First we note the fact that $\chi(g)$ must be an nth root of unity. This means there can at most be n such characters. In proposition 2.1.5 we found a character χ such that $\chi(g) = e^{\frac{2\pi i}{n}}$. Then by taking $\varepsilon, \chi, \chi^2, ..., \chi^{n-1}$ we get n distinct characters of order dividing n. □

Now we show the proposition. We consider the cases $a = 0$ and $a \neq 0$ separately. First we note that since $\mathbb{F}_p$ is a field, the case $a = 0$ has one solution, namely $x = 0$. We have $\sum_{\chi^n=\varepsilon} \chi(0) = 1$, since $\varepsilon(0) = 1$, and we have defined $\chi(0) = 0$ for $\chi \neq \varepsilon$.
For $a \neq 0$, $x^n = a$ is either solvable or not. If it is solvable, there is a $b \in \mathbb{F}_p^*$ such that $b^n = a$. For $\chi^n = \varepsilon$, we have that

$$\chi(a) = \chi(b^n) = \chi(b)^n = \chi^n(b) = \varepsilon(b) = 1.$$

This implies

$$N(x^n = a) = \sum_{\chi^n = \varepsilon} \chi(a) = n$$

as there are exactly n characters χ such that $\chi^n = \varepsilon$ by the preceding lemma. If $x^n = a$ is not solvable, we show that $\sum_{\chi^n=\varepsilon} \chi(a) = 0$. By proposition 2.1.5 there exists a character ρ such that $\rho(a) \neq 1$ and $\rho^n = \varepsilon$. Then we have that

$$\begin{aligned}
\rho(a) \sum_{\chi^n=\varepsilon} \chi(a) &= \sum_{\chi^n=\varepsilon} \rho(a)\chi(a) \\
&= \sum_{\chi^n=\varepsilon} \rho\chi(a) \\
&= \sum_{\chi^n=\varepsilon} \chi(a)
\end{aligned}$$

where the last equality follows from the fact that the characters of order dividing n form a group, and for fixed ρ, $\rho\chi$ runs through all these characters as χ does. Since $\rho(a) \neq 0$, we must have $\sum_{\chi^n=\varepsilon} \chi(a) = 0$ as wanted. This completes the proof. □

Lemma 2.1.8. *In the special case $n = 2$, we have $N(x^2 = a) = 1 + \left(\frac{a}{p}\right)$ where $\left(\frac{a}{p}\right)$ is the Legendre symbol.*

Proof. This follows by counting solutions; $a = 0$ gives one solution as mentioned above, and since $n = 2$, we only have one multiplicative character of order 2, namely $\chi(\cdot) = \left(\frac{\cdot}{p}\right)$. □

2.2 Gauss sums

After working with multiplicative characters, we are ready to define Gauss sums and consider their properties: let χ be a character on $\mathbb{F}_p$ as previously, and let a be an element of $\mathbb{F}_p$.

Definition 2.2.1. *We denote by $g_a(\chi)$ the Gauss sum corresponding to the character χ, where $g_a(\chi)$ is given by*

$$g_a(\chi) = \sum_{t \in \mathbb{F}_p} \chi(t) e^{at\frac{2i\pi}{p}}$$

for all a in $\mathbb{F}_p$.

For convenience we write $e^{\frac{2i\pi}{p}} = \zeta$, so that $e^{at\frac{2i\pi}{p}} = \zeta^{at}$. Furthermore, in the case $a = 1$, which we primarily work with, we use the abbreviation $g_1(\chi) = g(\chi)$. Now we are ready to formulate some useful results about Gauss sums, however first we need a few lemmas:

Lemma 2.2.2. *For $a \in \mathbb{F}_p^*$ we have*

$$\sum_{t=0}^{p-1} \zeta^{at} = p \text{ for } a \equiv 0 \mod p$$
$$\sum_{t=0}^{p-1} \zeta^{at} = 0 \text{ for } a \not\equiv 0 \mod p$$

Proof. If $a \equiv 0 \mod p$, then $\zeta^a = 1$ since $e^{2\pi i} = 1$. Then $\sum_{t=0}^{p-1} \zeta^{at} = p$. If $a \not\equiv 0 \mod p$ then $\zeta^a \neq 1$, and by the sum formula of the geometric series we have $\sum_{t=0}^{p-1} \zeta^{at} = \frac{\zeta^{ap}-1}{\zeta^a-1} = 0$, again since $e^{2\pi i} = 1$. □

This corollary follows immediately from the lemma:

Corollary 2.2.2.1. *For x and y in $\mathbb{F}_p$, define the delta function as $\delta(x, y) = 1$ for $x \equiv y \mod p$ and $\delta(x, y) = 0$ otherwise. Then we have*

$$\sum_{t=0}^{p-1} \zeta^{t(x-y)} = p\delta(x, y).$$

Proof. Simply substitute $a = x - y$ in the proof of lemma 2.2.2. □

Proposition 2.2.3. *For a in $\mathbb{F}_p$ and a character χ we have the following:*

a) For $a \neq 0$ and $\chi \neq \varepsilon$: $g_a(\chi) = \chi(a^{-1})g(\chi)$;

b) For $a \neq 0$ and $\chi = \varepsilon$: $g_a(\varepsilon) = 0$;

c) For $a = 0$ and $\chi = \varepsilon$: $g_0(\varepsilon) = p$;

d) For $a = 0$ and $\chi \neq \varepsilon$: $g_0(\chi) = 0$.

Proof. a) For $a \neq 0$ and $\chi \neq \varepsilon$, we have

$$\chi(a)g_a(\chi) = \chi(a)\sum_{t\in\mathbb{F}_p}\chi(t)\zeta^{at} = \sum_{t\in\mathbb{F}_p}\chi(at)\zeta^{at} = g(\chi)$$

since for fixed a,at runs over the elements of $\mathbb{F}_p$ as t does.
b) For $a \neq 0$,

$$g_a(\varepsilon) = \sum_{t\in\mathbb{F}_p}\varepsilon(t)\zeta^{at} = \sum_{t\in\mathbb{F}_p}\zeta^{at} = 0$$

by use of lemma 2.2.2.
c) We have

$$g_0(\varepsilon) = \sum_{t\in\mathbb{F}_p}\varepsilon(t)\zeta^{0t} = \sum_{t\in\mathbb{F}_p}\varepsilon(t) = p$$

by proposition 2.1.3.
d) By definition $g_0(\chi) = \sum\limits_{t\in\mathbb{F}_p}\chi(t)$. By proposition 2.1.3 this sum is equal to zero for $\chi \neq \varepsilon$. □

Proposition 2.2.4. *For $\chi \neq \varepsilon$ it holds that $|g(\chi)| = \sqrt{p}$.*

Proof. We proceed by considering the sum $\sum\limits_{a\in\mathbb{F}_p} g_a(\chi)\overline{g_a(\chi)}$. By proposition 2.2.3 a), we have that $\overline{g_a(\chi)} = \overline{\chi(a^{-1})g(\chi)} = \chi(a)\overline{g(\chi)}$ for $a \neq 0$. By using this, we have

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

since $\chi(a^{-1})\chi(a) = \underline{\chi(a^{-1}}a) = 1$. By proposition 2.2.3 d), $g_0(\chi) = 0$ for $\chi \neq \varepsilon$, so we have that $\sum\limits_{a\in\mathbb{F}_p} g_a(\chi)\overline{g_a(\chi)} = (p-1)|g(\chi)|^2$. By direct calculation we also have

$$g_a(\chi)\overline{g_a(\chi)} = \sum_{x\in\mathbb{F}_p}\sum_{y\in\mathbb{F}_p}\chi(x)\overline{\chi(y)}\zeta^{a(x-y)}.$$

Summing over $a \in \mathbb{F}_p$ on both sides gives:

$$\begin{aligned}\sum_{a\in\mathbb{F}_p} g_a(\chi)\overline{g_a(\chi)} &= \sum_{a\in\mathbb{F}_p}\sum_{x\in\mathbb{F}_p}\sum_{y\in\mathbb{F}_p}\chi(x)\overline{\chi(y)}\zeta^{a(x-y)} \\ &= \sum_{x\in\mathbb{F}_p}\sum_{y\in\mathbb{F}_p}\chi(x)\overline{\chi(y)}\delta(x,y)p \\ &= (p-1)p\end{aligned}$$

by use of corollary 2.2.2.1 in the second to last equality. By this we have that $(p-1)|g(\chi)|^2 = (p-1)p$, hence $|g(\chi)| = \sqrt{p}$. □

Lemma 2.2.5. *Recalling the definition of $\overline{\chi}$ as the character that takes $a \in \mathbb{F}_p$ to $\overline{\chi(a)} = \chi(a)^{-1}$, we have $\overline{g(\chi)} = \chi(-1)g(\overline{\chi})$. Furthermore, $g(\chi)g(\overline{\chi}) = \chi(-1)p$.*

Proof. We calculate the conjugated Gauss sum as

$$\overline{g(\chi)} = \sum_{t\in\mathbb{F}_p} \overline{\chi(t)\zeta^t} = \sum_{t\in\mathbb{F}_p} \overline{\chi(t)}\zeta^{-t} = \chi(-1)\sum_{t\in\mathbb{F}_p} \overline{\chi(-t)}\zeta^{-t} = \chi(-1)g(\overline{\chi}).$$

Here we have used that $\overline{\chi(-1)} = \chi(-1)$, since we must have $\chi(-1) = \pm 1$. From this we can also remark that $|g(\chi)|^2 = p$ is equivalent to $g(\chi)g(\overline{\chi}) = \chi(-1)p$. □

After studying the properties of Gauss sums, we are ready to introduce another type of character sum, namely Jacobi sums, which we will use extensively to analyse solutions to various types of equations.

2.3 Jacobi sums

Let χ and λ be characters on $\mathbb{F}_p$ and denote by $J(\chi, \lambda)$ the sum

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

for a and b in $\mathbb{F}_p$. We call this type of sum a Jacobi sum. Like in the case of Gauss sums, we start by introducing some useful properties of Jacobi sums, and then we will apply these to the study of equations over $\mathbb{F}_p$.

Theorem 2.3.1. *Let $\chi \neq \varepsilon$ and $\lambda \neq \varepsilon$ be characters on $\mathbb{F}_p$. Then the following hold:*

a) $J(\varepsilon,\varepsilon) = p$;

b) $J(\varepsilon,\chi) = 0$;

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

d) for $\chi\lambda \neq \varepsilon$, $J(\chi,\lambda) = \frac{g(\chi)g(\lambda)}{g(\lambda\chi)}$.

Proof. a) Since

$$J(\varepsilon,\varepsilon) = \sum_{a+b=1} \varepsilon(a)\varepsilon(b) = \sum_{a+b=1} \varepsilon(ab)$$

this is trivially equal to p by definition of ε (recall we have defined the extension $\varepsilon(0) = 1$).
b) This follows by proposition 2.1.3, since by definition of ε,

$$\sum_{a+b=1} \varepsilon(a)\chi(b) = \sum_{b\in\mathbb{F}_p} \chi(b) = 0.$$

c) First note that:

$$J(\chi,\chi^{-1}) = \sum_{a+b=1} \chi(a)\chi^{-1}(b) = \sum_{\substack{a+b=1\\ b\neq 0}} \chi\left(\frac{a}{b}\right) = \sum_{a\neq 1} \chi\left(\frac{a}{1-a}\right)$$

where we have substituted $b = 1-a$ in the last step. Note that the $b = 0$ term is zero, and this is the term where $a = 1$. If we let $c = \frac{a}{1-a}$, then for $c \neq -1$, $a = \frac{c}{1+c}$. Hence as

a runs through the elements of $\mathbb{F}_p\backslash\{1\}$, c runs through the elements of $\mathbb{F}_p\backslash\{-1\}$. So we have

$$J(\chi,\chi^{-1})+\chi(-1)=\left(\sum_{c\neq -1}\chi(c)\right)=0$$

by proposition 2.1.3, and hence $J(\chi,\chi^{-1})=-\chi(-1)$.
d) First we observe that

$$\begin{aligned} g(\chi)g(\lambda) &= \left(\sum_{t\in\mathbb{F}_p}\chi(t)\zeta^t\right)\left(\sum_{s\in\mathbb{F}_p}\lambda(s)\zeta^s\right) \\ &= \sum_{t\in\mathbb{F}_p}\sum_{s\in\mathbb{F}_p}\chi(t)\lambda(s)\zeta^{t+s} \\ &= \sum_{u\in\mathbb{F}_p}\left(\sum_{t+s=u}\chi(t)\lambda(s)\right)\zeta^u. \end{aligned}$$

If $u=t+s=0$ then $t=-s$ (or $s=-t$) and we get

$$\begin{aligned} g(\chi)g(\lambda) &= \sum_{t+s=0}\chi(t)\lambda(s)=\sum_{t\in\mathbb{F}_p}\chi(t)\lambda(-t) \\ &= \lambda(-1)\sum_{t\in\mathbb{F}_p}\chi\lambda(t)=0 \end{aligned}$$

by proposition 2.1.3 since by assumption $\chi\lambda\neq\varepsilon$. If $u=t+s\neq 0$, define t' and s' by $t=ut'$ and $s=us'$. These s' and t' exist since $\mathbb{F}_p$ is a field. Then for $t+s=u$, $t'+s'=1$. From this we get

$$\sum_{t+s=u}\chi(t)\lambda(s)=\sum_{t'+s'=1}\chi(ut')\lambda(us')=\chi(u)\lambda(u)\sum_{t'+s'=1}\chi(t')\lambda(s')=\chi\lambda(u)J(\chi,\lambda).$$

Then by substitution, we have

$$\begin{aligned} g(\chi)g(\lambda) &= \sum_{u\in\mathbb{F}_p}\left(\sum_{t+s=u}\chi(t)\lambda(s)\right)\zeta^u \\ &= \sum_{u\in\mathbb{F}_p}\chi\lambda(u)J(\chi,\lambda)\zeta^u \\ &= g(\chi\lambda)J(\chi,\lambda) \end{aligned}$$

and so $J(\chi,\lambda)=\frac{g(\chi)g(\lambda)}{g(\chi\lambda)}$. Note that is is well-defined since $g(\chi\lambda)\neq 0$ by proposition 2.2.3 a) This completes the theorem. □

Corollary 2.3.1.1. *If $\chi\neq\varepsilon$, $\lambda\neq\varepsilon$ and $\chi\lambda\neq\varepsilon$, then $|J(\chi,\lambda)|=\sqrt{p}$.*

Proof. We use theorem 2.3.1 d) and take the absolute value:

$$|J(\chi,\lambda)|=\Big|\frac{g(\chi)g(\lambda)}{g(\chi\lambda)}\Big|.$$

We then apply proposition 2.2.4 (since all involved characters are non-trivial):

$$|J(\chi, \lambda)| = \left|\frac{\sqrt{p}\sqrt{p}}{\sqrt{p}}\right| = |\sqrt{p}| = \sqrt{p}.$$

□

Proposition 2.3.2. *For $p \equiv 1 \mod n$ and χ a character of order n, $n > 2$, we have that*

$$g(\chi)^n = \chi(-1)pJ(\chi, \chi)J(\chi, \chi^2) \cdot \ldots \cdot J(\chi, \chi^{n-2}).$$

Proof. using theorem 2.3.1 d), we have that $g(\chi)^2 = J(\chi, \chi)g(\chi^2)$. We multiply both sides by $g(\chi)$:

$$\begin{aligned} g(\chi)^3 &= g(\chi)^2 g(\chi) \\ &= J(\chi, \chi)g(\chi^2)g(\chi) \\ &= J(\chi, \chi)J(\chi, \chi^2)g(\chi^3) \end{aligned}$$

since $J(\chi, \chi^2) = \frac{g(\chi^2)g(\chi)}{g(\chi^3)}$. Continuing this successively, we have that

$$g(\chi)^{n-1} = J(\chi, \chi)J(\chi, \chi^2) \cdot \ldots \cdot J(\chi, \chi^{n-2})g(\chi^{n-1}).$$

Since χ has order n, we have $\chi^{n-1} = \chi^{-1} = \overline{\chi}$, so that $g(\chi)g(\chi^{n-1}) = g(\chi)g(\overline{\chi}) = \chi(-1)p$ by lemma 2.2.5. By multiplying both sides by $g(\chi)$, we get

$$\begin{aligned} g(\chi)^n &= g(\chi)g(\chi)^{n-1} \\ &= J(\chi, \chi)J(\chi, \chi^2) \cdot \ldots \cdot J(\chi, \chi^{n-2})g(\chi^{n-1})g(\chi) \\ &= \chi(-1)pJ(\chi, \chi)J(\chi, \chi^2) \cdot \ldots \cdot J(\chi, \chi^{n-2}) \end{aligned}$$

by lemma 2.2.5, since $g(\chi^{n-1})g(\chi) = g(\chi^{-1})g(\chi) = g(\overline{\chi})g(\chi) = \chi(-1)p$. This gives the desired result. □

Corollary 2.3.2.1. *For χ a character of order 3 (also called a cubic character) and $p \equiv 1 \mod 3$, we have $g(\chi)^3 = pJ(\chi, \chi)$.*

Proof. This follows from proposition 2.3.2 and putting $n = 3$, and observing that $\chi(-1) = \chi((-1)^3) = \chi(-1)^3 = 1$. □

Having worked with Jacobi sums and understanding their properties, we will now start implementing this theory in the study of concrete equations over finite fields. We will first consider a small example that can be analysed directly using Jacobi sums, then we will move on to more complex cases that also require number theoretical methods.

Example 2.3.3.

We now look at an example of the application of Jacobi sums. Let p be an odd prime, $p \equiv 1 \mod 4$, and let χ be a multiplicative character of order 4 on $\mathbb{F}_p$. Let $\rho(\cdot) = \left(\frac{\cdot}{p}\right)$ and $J(\chi, \rho) = a + ib$. We wish to find the number of solutions over $\mathbb{F}_p$ to

$$y^2 + x^4 = 1.$$

We have that

$$\begin{aligned} N(y^2+x^4=1) &= \sum_{a+b=1} N(y^2=a)N(x^4=b) \\ &= \sum_{a+b=1}\left((1+\rho(a))\sum_{j=0}^{3}\lambda^j(b)\right) \end{aligned}$$

by lemma 2.1.8 and proposition 2.1.6, where the inner sum is over all characters λ of order dividing 3. By expanding we get

$$\begin{aligned} & \sum_{a+b=1}\sum_{j=0}^{3}\lambda^j(b) + \sum_{a+b=1}\sum_{j=0}^{3}\lambda^j(b)\rho(a) \\ = \; & J(\lambda^0,\varepsilon)+J(\lambda,\varepsilon)+J(\lambda^2,\varepsilon)+J(\lambda^3,\varepsilon)+J(\lambda^0,\rho)+J(\lambda,\rho)+J(\lambda^2,\rho)+J(\lambda^3,\rho) \\ = \; & p+0+0+0+0+J(\lambda,\rho)+J(\lambda^2,\rho)+J(\lambda^3,\rho) \\ = \; & p+J(\lambda,\rho)+J(\rho,\rho)+J(\lambda^{-1},\rho) \\ = \; & p+J(\lambda,\rho)+J(\rho,\rho)+J(\overline{\lambda},\rho) \\ = \; & p+a+ib+a-ib+J(\rho,\rho) \\ = \; & p-(-1)^{\frac{p-1}{2}}+2a \\ = \; & p-1+2a \end{aligned}$$

where we have used theorem 2.3.1 and the following observations: $\lambda^2=\rho$ (since λ^2 has order 2 so this character is uniquely determined); $\overline{J(\lambda,\rho)}=J(\overline{\lambda},\overline{\rho})=J(\overline{\lambda},\rho)$ (since ρ is the Legendre symbol); $J(\rho,\rho)=J(\rho,\rho^{-1})=-\rho(-1)=-(-1)^{\frac{p-1}{2}}$ (again as ρ is the Legendre symbol) and finally $\lambda^3=\lambda^{-1}=\overline{\lambda}$.
Hence $N(y^2+x^4=1)=p-1+2a$.

The cardinality of the solution sets: some specific cases with 2 variables

We will now consider three slightly more complicated cases. These will illustrate how useful character theory and Jacobi sums are in the study of different types of equations.

3.1 The equation $x_1^2 + x_2^2 = 1$ over $\mathbb{F}_p$

We first look at the familiar equation $x_1^2 + x_2^2 = 1$ over $\mathbb{F}_p$. Since we are working over a finite field, $x_1^2 + x_2^2 = 1$ can only have finitely many solutions. Recall that $N(x_1^2 + x_2^2 = 1)$ denotes the number of solutions over $\mathbb{F}_p$. We will now show how to find this number explicitly. We wish to show

Proposition 3.1.1.

$$\begin{aligned} N(x_1^2 + x_2^2 = 1) &= p - 1,\ p \equiv 1 \mod 4 \\ N(x_1^2 + x_2^2 = 1) &= p + 1,\ p \equiv 3 \mod 4. \end{aligned}$$

Proof. First observe that

$$N(x_1^2 + x_2^2 = 1) = \sum_{a+b=1} N(x_1^2 = a) N(x_2^2 = b)$$

where we sum over all pairs a and b in $\mathbb{F}_p$ such that $a + b = 1$. By lemma 2.1.8, we have that

$$N(x_1^2 + x_2^2 = 1) = p + \sum_{a \in \mathbb{F}_p} \left(\frac{a}{p}\right) + \sum_{b \in \mathbb{F}_p} \left(\frac{b}{p}\right) + \sum_{a+b=1} \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

We know that the first two sums are zero by proposition 2.1.3. We apply theorem 2.3.1 c) to the last sum and get

$$\begin{aligned} \sum_{a+b=1} \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) &= \sum_{a+b=1} \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)^{-1} = \sum_{a+b=1} \chi(a)\chi^{-1}(b) \\ &= J(\chi, \chi^{-1}) = -\chi(-1) = -(-1)^{\frac{p-1}{2}} \end{aligned}$$

by definition of the Legendre symbol. We have used the fact that for any b in $\mathbb{F}_p$, $\chi(b) = \left(\frac{b}{p}\right) = \left(\frac{b}{p}\right)^{-1} = \chi(b)^{-1}$, since the Legendre symbol is always equal to ±1, which is unaffected by taking the reciprocal. From this, we get that

$$\begin{aligned} N(x_1^2+x_2^2=1) &= p-1,\ p\equiv 1 \mod 4 \\ N(x_1^2+x_2^2=1) &= p+1,\ p\equiv 3 \mod 4 \end{aligned}$$

since we know from number theory that $\chi(-1)=\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}$ is 1 for $p\equiv 1 \mod 4$ and -1 for $p\equiv 3 \mod 4$. □

3.2 The equation $x_1^3+x_2^3=1$ over $\mathbb{F}_p$

We now wish to consider the number $N(x_1^3+x_2^3=1)$. This is only a small change in exponents when we compare the previous case, however already at this stage our computations become more complicated. Decomposing our equation into Jacobi sums does not allow us to compute $N(x_1^3+x_2^3=1)$ directly, however it will give us a very informative bound on the number of solutions. We will show the following result:

Proposition 3.2.1. *Over $\mathbb{F}_p$ the number of solutions to the equation $x_1^3+x_2^3=1$ is given by*

$$N(x_1^3+x_2^3=1) \quad = \quad p-2+2ReJ(\chi,\chi)$$

where χ is a cubic character on $\mathbb{F}_p$.

Proof. We can decompose this into the sum

$$N(x_1^3+x_2^3=1)=\sum_{a+b=1} N(x_1^3=a)N(x_2^3=b).$$

First we show the following lemma:

Lemma 3.2.2. *If $p\equiv 2 \mod 3$, then $N(x^3=a)=1$.*

Proof. If $p\equiv 2 \mod 3$ then $p-1\equiv 1 \mod 3$, hence $3 \not| p-1$. This means that when we consider residue classes in $\mathbb{F}_p$, we have that $\{1,...,p-1\}=\{1^3,...,(p-1)^3\}$. Hence the map $x\mapsto x^3$ is a bijection, which precisely means that $N(x^3=a)=1$. □

Assume now that $p\equiv 1 \mod 3$. Let $\chi\neq\varepsilon$ be a character of order 3, then χ^2 also has order 3 so $\chi^2\neq\varepsilon$. Since there are exactly 3 characters of order 3, these are ε,χ and χ^2. These are the cubic characters over $\mathbb{F}_p$. By proposition 2.1.6, we have that

$$N(x^3=a)=1+\chi(a)+\chi^2(a).$$

Hence we get

$$\begin{aligned} N(x_1^3+x_2^3=1) &= \sum_{a+b=1}\sum_{i=0}^{2}\sum_{j=0}^{2}\chi^i(a)\chi^j(b) \\ &= \sum_{i=0}^{2}\sum_{j=0}^{2}\sum_{a+b=1}\chi^i(a)\chi^j(b). \end{aligned}$$

By writing out this sum, we get

$$\begin{aligned}\sum_{i=0}^{2}\sum_{j=0}^{2}\sum_{a+b=1}\chi^i(a)\chi^j(b) &= \sum_{a+b=1}\chi^0(a)\chi^0(b)+\sum_{a+b=1}\chi^0(a)\chi(b)+\sum_{a+b=1}\chi^0(a)\chi^2(b)\\ &+ \sum_{a+b=1}\chi(a)\chi^0(b)+\sum_{a+b=1}\chi(a)\chi(b)+\sum_{a+b=1}\chi(a)\chi^2(b)\\ &+ \sum_{a+b=1}\chi^2(a)\chi^0(b)+\sum_{a+b=1}\chi^2(a)\chi(b)+\sum_{a+b=1}\chi^2(a)\chi^2(b).\end{aligned}$$

When we use the results of theorem 2.3.1, we find this to be

$$\begin{aligned}\sum_{i=0}^{2}\sum_{j=0}^{2}\sum_{a+b=1}\chi^i(a)\chi^j(b) &= p+0+0+0+J(\chi,\chi)+J(\chi,\chi^2)+0+J(\chi^2,\chi)+J(\chi^2,\chi^2)\\ &= p+J(\chi,\chi)+J(\chi,\chi^{-1})+J(\chi^{-1},\chi)+J(\chi^2,\chi^2)\\ &= p+J(\chi,\chi)+J(\chi^{-1},\chi^{-1})-\chi(-1)-\chi^2(-1).\end{aligned}$$

Since χ has order 3, $\chi^2=\chi^{-1}=\overline{\chi}$. By linearity of Jacobi sums, $J(\overline{\chi},\overline{\chi^{-1}})=\overline{J(\chi,\chi^{-1})}$ since we have

$$\overline{J(\chi,\lambda)}=\overline{\sum_{a+b=1}\chi(a)\lambda(b)}=\sum_{a+b=1}\overline{\chi(a)\lambda(b)}=\sum_{a+b=1}\overline{\chi(a)}\;\overline{\lambda(b)}=J(\overline{\chi},\overline{\lambda}).$$

This means that $J(\chi^{-1},\chi)=\overline{J(\chi,\chi^{-1})}=\overline{-\chi(-1)}=-\chi^2(-1)$, which gives the last term and that $J(\chi^{-1},\chi^{-1})=\overline{J(\chi,\chi)}$. Finally by observing that $-1=(-1)^3$ so $\chi(-1)=\chi(-1)^3=1$ we find the result

$$N(x_1^3+x_2^3=1) \;=\; p-2+2ReJ(\chi,\chi).$$

□

By use of corollary 2.3.1.1, we also have the estimate

$$|N(x_1^3+x_2^3=1)-p+2|\leq|2ReJ(\chi,\chi)|\leq 2|ReJ(\chi,\chi)|\leq 2|J(\chi,\chi)|=2\sqrt{p}$$

since we recall that the modulus of a complex number is always greater than the absolute value of its real part. In plain terms, this estimate tells us that the number of solutions $N(x_1^2+x_2^2=1)$ differs from $p-2$ by at most $2\sqrt{p}$. In other words, for suitably large prime p, we know there are many solutions, even if we do not know the precise number.

3.3 The equation $x_1^n+x_2^n=1$ over $\mathbb{F}_p$

The last case in two variables that we consider here is the equation $x_1^n+x_2^n=1$ over $\mathbb{F}_p$. As in the previous case, we will use Jacobi sums to find a bound on the number of solutions. More specifically, we will show:

Proposition 3.3.1. *Let $p \equiv 1 \mod n$. Then then number of solutions to $x_1^n + x_2^n = 1$, $n \in \mathbb{N}$, in $\mathbb{F}_p$ is given by*

$$N(x_1^n + x_2^n = 1) = p + 1 - \delta_n(-1)n + \sum_{\substack{i,j=1 \\ i+j \neq n}}^{n-1} J(\chi^i, \chi^j)$$

where $\delta_n(-1) = 1$ for $-1 = \alpha^n$ for some α in $\mathbb{F}_p$ and $\delta_n(-1) = 0$ otherwise.

Proof. We use the decomposition

$$N(x_1^n + x_2^n = 1) = \sum_{a+b=1} N(x_1^n = a)N(x_2^n = b).$$

Let χ be a character of order n. From proposition 2.1.6 we know that $N(x_1^n = a) = \sum\limits_{j=0}^{n-1} \chi^j(a)$ (similarly for x_2), and by this we get

$$N(x_1^n + x_2^n = 1) = \sum_{a+b=1} \sum_{j=0}^{n-1} \sum_{i=0}^{n-1} \chi^j(a)\chi^i(b) = \sum_{j=0}^{n-1} \sum_{i=0}^{n-1} J(\chi^j, \chi^i).$$

We apply theorem 2.3.1. For $i = j = 0$, $J(\chi^0, \chi^0) = p$ since $\chi^0 = \varepsilon$. For $j + i = n$, we have that

$$J(\chi^j, \chi^i) = J(\chi^j, \chi^{n-j}) = J(\chi^j, \chi^n \chi^{-j}) = J(\chi^j, (\chi^j)^{-1}) = -\chi^j(-1)$$

and these terms sum to $-\sum\limits_{j=1}^{n-1} \chi^j(-1)$. We note that $\sum\limits_{j=0}^{n-1} \chi^j(-1) = n$ for -1 an nth power (i.e. $-1 = \alpha^n$ for some $\alpha \in \mathbb{F}_p$) and $\sum\limits_{j=0}^{n-1} \chi^j(-1) = 0$ otherwise. Hence these terms contribute $1 - \delta_n(-1)n$, where $\delta_n(-1) = 1$ for -1 an nth power and $\delta_n(-1) = 0$ otherwise. The last case to consider is where $i = 0$ and $j \neq 0$, or $j = 0$ and $i \neq 0$. This case gives that $J(\chi^i, \chi^j) = 0$. So in total, we get

$$N(x_1^n + x_2^n = 1) = p + 1 - \delta_n(-1)n + \sum_{\substack{i,j=1 \\ i+j \neq n}}^{n-1} J(\chi^i, \chi^j).$$

This proves the proposition. □

Lastly, we note that $\sum\limits_{\substack{i,j=1 \\ i+j \neq n}}^{n-1} J(\chi^i, \chi^j) = (n-1)^2 - (n-1) = (n-1)(n-2)$, all with absolute value $\sqrt{p}$ by corollary 2.3.1.1. From this, we directly get the following result on the absolute value:

Proposition 3.3.2. *We have the following bound on $N(x_1^2 + x_2^2 = 1)$:*

$$|N(x_1^n + x_2^n = 1) + \delta_n(-1)n - (p+1)| \leq (n-1)(n-2)\sqrt{p}.$$

Proof. This follows immediately by the above. □

Generalized Jacobi sums

In the previous chapter we saw how much information about different equations we could derive using primarily the properties of Jacobi sums. Up to now we have only been working with Jacobi sums defined for two characters, i.e. of the form $J(\chi, \lambda)$. We will see that when studying more complicated equations with different parameters, it is useful to expand our previous results for Jacobi sums to cases with more characters.

Definition 4.0.1. *Let $\chi_1, ..., \chi_l$ be characters on $\mathbb{F}_p$. Then a multi-character Jacobi sum is given by*

$$J(\chi_1, ..., \chi_l) = \sum_{t_1+...+t_l=1} \chi_1(t_1)\chi_2(t_2) \cdot ... \cdot \chi_l(t_l), \ t_i \in \mathbb{F}_p.$$

Note that the case $l = 2$ is simply the case we studied in chapter 3. It is also useful to introduce another variant of multi-character Jacobi sums, namely J_0, which is simply the case where $\sum\limits_{i=1}^{l} t_i = 0$:

$$J_0(\chi_1, ..., \chi_l) = \sum_{t_1+...+t_l=0} \chi_1(t_1) \cdot ... \cdot \chi_l(t_l).$$

Let us begin by extending our previous theorem 2.3.1 to the multi-character case:

Theorem 4.0.2. *For χ_i, $i = 1, ..., l$, characters on $\mathbb{F}_p$ and ε the trivial character, the following hold:*

a) $J_0(\varepsilon, \varepsilon, ..., \varepsilon) = J(\varepsilon, \varepsilon, ..., \varepsilon) = p^{l-1}$;

b) If for some, but not all i, χ_i is trivial, then $J_0(\chi_1, \chi_2, ..., \chi_l) = J(\chi_1, \chi_2, ..., \chi_l) = 0$;

c) Let $\chi_l \neq \varepsilon$. Then $J_0(\chi_1, \chi_2, ..., \chi_l) = 0$ for $\chi_1\chi_2 \cdot ... \cdot \chi_l \neq \varepsilon$, and

$$J_0(\chi_1, ..., \chi_l) = \chi_l(-1)(p-1)J(\chi_1, \chi_2, ..., \chi_{l-1})$$

otherwise.

Proof. a) For $t_1, t_2, ..., t_{l-1}$ chosen arbitrarily in $\mathbb{F}_p$, t_l is uniquely determined by the equation $t_1 + t_2 + ... + t_{l-1} + t_l = 0$, hence $J_0(\varepsilon, \varepsilon, ..., \varepsilon) = p^{l-1}$. Similarly for arbitrary $t_1, ..., t_{l-1}$, t_l is uniquely determined by the equation $t_1 + ... + t_l = 1$, hence $J(\varepsilon, ..., \varepsilon) = p^{l-1}$.

b) Assume that $\chi_i, i = 1, ..., s$ are non-trivial, and that $\chi_j = \varepsilon$ for $j = s+1, ..., l$. Then we have that

$$\begin{aligned}\sum_{t_1+...+t_l=0} \chi_1(t_1) \cdot ... \cdot \chi_l(t_l) &= \sum_{t_1,...,t_{l-1} \in \mathbb{F}_p} \chi_1(t_1) \cdot ... \cdot \chi_s(t_s) \\ &= p^{l-s-1} \left(\sum_{t_1 \in \mathbb{F}_p} \chi_1(t_1) \right) \cdot ... \cdot \left(\sum_{t_s \in \mathbb{F}_p} \chi_s(t_s) \right) \\ &= 0\end{aligned}$$

where in the last step we apply proposition 2.1.3.
c) First we note that

$$J_0(\chi_1, \chi_2, ..., \chi_l) = \sum_{s \in \mathbb{F}_p} \left(\sum_{t_1+...+t_{l-1}=-s} \chi_1(t_1) \cdot ... \cdot \chi_{l-1}(t_{l-1}) \right) \chi_l(s).$$

Since by assumption $\chi_l \neq \varepsilon$, we have $\chi_l(0) = 0$. This means we can assume $s \neq 0$ in the sum above. For $s \neq 0$ we define t_i' by the identity $t_i = -st_i'$. This is possible since $\mathbb{F}_p$ is a field. Then we have

$$\begin{aligned}\sum_{t_1+....+t_{l-1}=-s} \chi_1(t_1) \cdot ... \cdot \chi_{l-1}(t_{l-1}) &= \chi_1\chi_2 \cdot ... \cdot \chi_{l-1}(-s) \sum_{t_1'+...+t_{l-1}'=1} \chi_1(t_1') \cdot ... \cdot \chi_{l-1}(t_{l-1}') \\ &= \chi_1\chi_2 \cdot ... \cdot \chi_{l-1}(-s) J(\chi_1, ..., \chi_{l-1}).\end{aligned}$$

By this we get

$$J_0(\chi_1, \chi_2, ..., \chi_l) = \chi_1\chi_2 \cdot ... \cdot \chi_{l-1}(-1) J(\chi_1, ..., \chi_{l-1}) \sum_{0 \neq s \in \mathbb{F}_p} \chi_1\chi_2 \cdot ... \cdot \chi_l(s)$$

because $\chi_1 \cdot ... \cdot \chi_l$ runs over the elements of $\mathbb{F}_p^*$ same as χ_l does (by assumption $\chi_1 \cdot ... \cdot \chi_l \neq \varepsilon$). Note that $\sum_{s \neq 0} \chi_1\chi_2 \cdot ... \cdot \chi_l(s) = 0$ if $\chi_1 \cdot ... \cdot \chi_l \neq \varepsilon$ by proposition 2.1.3 and $\sum_{s \neq 0} \chi_1\chi_2 \cdot ... \cdot \chi_l(s) = p - 1$ if $\chi_1 \cdot ... \cdot \chi_l = \varepsilon$. This gives c). □

We also have the following theorem that shows the connection between multi-character Jacobi sums and Gauss sums:

Theorem 4.0.3. *Let χ_i, $i = 1, ..., r$, be non-trivial characters, and let $\chi_1 \cdot ... \cdot \chi_l \neq \varepsilon$. Then we have the relation*

$$g(\chi_1)g(\chi_2) \cdot ... \cdot g(\chi_r) = J(\chi_1, ..., \chi_r) g(\chi_1\chi_2 \cdot ... \cdot \chi_r)$$

so in particular

$$J(\chi_1, ..., \chi_r) = \frac{g(\chi_1)g(\chi_2) \cdot ... \cdot g(\chi_r)}{g(\chi_1\chi_2 \cdot ... \cdot \chi_r)}.$$

Proof. First define the map $\varphi : \mathbb{F}_p \to \mathbb{C}$ by $\varphi(t) = \zeta^t$, where we recall that $\zeta = e^{\frac{2i\pi}{p}}$. Note that $\varphi(t_1 + t_2) = \varphi(t_1)\varphi(t_2)$ and $g(\chi) = \sum\limits_{t \in \mathbb{F}_p} \chi(t)\varphi(t)$. Then we have that

$$\begin{aligned} g(\chi_1) \cdot ... \cdot g(\chi_r) &= \left(\sum_{t_1 \in \mathbb{F}_p} \chi(t_1)\varphi(t_1) \right) \cdot ... \cdot \left(\sum_{t_r \in \mathbb{F}_p} \chi(t_r)\varphi(t_r) \right) \\ &= \sum_{s \in \mathbb{F}_p} \left(\sum_{t_1 + ... + t_r = s} \chi_1(t_1) \cdot ... \cdot \chi_r(t_r) \right) \varphi(s). \end{aligned}$$

We consider the case $s = 0$ and the case $s \neq 0$: for $s = 0$, then since $\chi_1 \cdot ... \cdot \chi_r \neq \varepsilon$, theorem 4.0.2 gives that

$$J_0(\chi_1, ..., \chi_r) = \sum_{t_1 + ... + t_r = 0} \chi_1(t_1) \cdot ... \cdot \chi_r(t_r) = 0.$$

For $s \neq 0$, we again use the substitution $t_i = st_i'$, $i = 1, .., r$, which gives that

$$\begin{aligned} \sum_{t_1 + ... t_r = s} \chi_1(t_1) \cdot ... \cdot \chi_r(t_r) &= \chi_1 \cdot ... \cdot \chi_r(s) \sum_{t_1' + ... t_r' = 1} \chi_1(t_1') \cdot ... \cdot \chi_r(t_r') \\ &= \chi_1 \cdot ... \cdot \chi_r(s) J(\chi_1, ..., \chi_r). \end{aligned}$$

Combining these, we have that

$$\begin{aligned} g(\chi_1) \cdot ... \cdot g(\chi_r) &= \sum_{0 \neq s \in \mathbb{F}_p} \chi_1 \cdot ... \cdot \chi_r(s) J(\chi_1, ..., \chi_r)\varphi(s) \\ &= J(\chi_1, ..., \chi_r) g(\chi_1 ... \chi_r) \end{aligned}$$

which is what we wanted to show. □

This theorem also has the following useful corollaries:

Corollary 4.0.3.1. *Let $\chi_i \neq \varepsilon$ and $\chi_1 \cdot ... \cdot \chi_r = \varepsilon$. Then we have that*

$$g(\chi_1) \cdot ... \cdot g(\chi_r) = \chi_r(-1) p J(\chi_1, ..., \chi_{r-1}).$$

Furthermore, it holds that

$$g(\chi_1 \cdot ... \cdot \chi_{r-1}) g(\chi_r) = \chi_r(-1)p.$$

Proof. By theorem 4.0.3 we have

$$g(\chi_1) \cdot ... \cdot g(\chi_{r-1}) = J(\chi_1, ..., \chi_{r-1}) g(\chi_1 \cdot ... \cdot \chi_{r-1}).$$

By multiplying both sides by $g(\chi_r)$, we have that

$$g(\chi_1) \cdot ... \cdot g(\chi_{r-1}) g(\chi_r) = J(\chi_1, ..., \chi_{r-1}) g(\chi_1 \cdot ... \cdot \chi_{r-1}) g(\chi_r)$$

since $\chi_1 \cdot ... \cdot \chi_{r-1}\chi_r = \varepsilon$, $\chi_1 \cdot ... \cdot \chi_{r-1} = \chi_r^{-1}$ and thus

$$g(\chi_1 \cdot ... \cdot \chi_{r-1}) g(\chi_r) = g(\chi_r^{-1}) g(\chi_r) = \chi_r(-1)p$$

by lemma 2.2.5. Inserting in the previous expression gives the result. □

Corollary 4.0.3.2. *Let $\chi_i \neq \varepsilon$ and $\chi_1 \cdot ... \cdot \chi_r = \varepsilon$. Then we have that*

$$J(\chi_1, ..., \chi_r) = -\chi_r(-1)J(\chi_1, ..., \chi_{r-1}).$$

If $r = 2$ we put $J(\chi_1) = 1$.

Proof. For $r = 2$, this is theorem 2.3.1 c). Now assume $r > 2$. We follow the proof of theorem 4.0.3 with the assumption that $\chi_1 \cdot ... \cdot \chi_r = \varepsilon$. Then we have that

$$\begin{aligned} g(\chi_1) \cdot ... \cdot g(\chi_r) &= J_0(\chi_1, ..., \chi_r)\chi_1 \cdot ... \cdot \chi_r(0) + J(\chi_1, ..., \chi_r) \sum_{s \neq 0} \chi_1 \cdot ... \cdot \chi_r(s)\varphi(s) \\ &= J_0(\chi_1, ..., \chi_r) + J(\chi_1, ..., \chi_r) \sum_{s \neq 0} \varphi(s) \end{aligned}$$

since $\chi_1 \cdot ... \cdot \chi_r(0) = \varepsilon(0) = 1$ and $\chi_1 \cdot ... \cdot \chi_r(s) = \varepsilon(s) = 1$. Since $\sum_{s \in \mathbb{F}_p} \varphi(s) = 0$, $-1 = -e^{\frac{2i\pi}{p}0} = -\varphi(0) = \sum_{s \neq 0} \varphi(s)$, hence

$$\begin{aligned} g(\chi_1) \cdot ... \cdot g(\chi_r) &= J_0(\chi_1, ..., \chi_r) - J(\chi_1, ..., \chi_r) \\ &= \chi_r(-1)(p-1)J(\chi_1, ..., \chi_{r-1}) - J(\chi_1, ..., \chi_r) \end{aligned}$$

by theorem 4.0.2 c). By the previous corollary, we also have that

$$g(\chi_1) \cdot ... \cdot g(\chi_r) = \chi_r(-1)pJ(\chi_1, ..., \chi_{r-1}).$$

By this we get

$$\chi_r(-1)pJ(\chi_1, ..., \chi_{r-1}) = \chi_r(-1)(p-1)J(\chi_1, ..., \chi_{r-1}) - J(\chi_1, ..., \chi_r)$$

so that

$$\begin{aligned} J(\chi_1, ..., \chi_r) &= \chi_r(-1)J(\chi_1, ..., \chi_{r-1})(p - 1 - p) \\ &= -\chi_r(-1)J(\chi_1, ..., \chi_{r-1}) \end{aligned}$$

as wanted. □

Finally, before moving on to the study of more complicated equations, we give one last theorem about multi-character Jacobi sums:

Theorem 4.0.4. *Let $\chi_i \neq \varepsilon, i = 1, ..., r$. Then we have that:*
a) for $\chi_1 \cdot ... \cdot \chi_r \neq \varepsilon$, $|J(\chi_1, ..., \chi_r)| = p^{\frac{r-1}{2}}$;
b) for $\chi_1 \cdot ... \cdot \chi_r = \varepsilon$, $|J_0(\chi_1, ..., \chi_r)| = (p-1)p^{\frac{r-2}{2}}$ and $|J(\chi_1, ..., \chi_r)| = p^{\frac{r-2}{2}}$.

Proof. a) By proposition 2.2.4 we have $|g(\chi)| = \sqrt{p}$. By theorem 4.0.3 we have

$$|J(\chi_1, ..., \chi_r)| = \left|\frac{g(\chi_1) \cdot ... \cdot g(\chi_r)}{g(\chi_1 \cdot ... \cdot \chi_r)}\right| = \left|\frac{\sqrt{p}^r}{\sqrt{p}}\right| = p^{\frac{r-1}{2}}.$$

b) By theorem 4.0.2 c) we have

$$|J_0(\chi_1, ..., \chi_r)| = |\chi_r(-1)(p-1)J(\chi_1, ..., \chi_{r-1})| = (p-1)p^{\frac{r-2}{2}}$$

which gives the first part. Corollary 4.0.3.2 gives that

$$|J(\chi_1, ..., \chi_r)| = |-\chi_r(-1)J(\chi_1, ..., \chi_{r-1})| = p^{\frac{r-2}{2}}$$

by part a). This completes the proof. □

Determining $N(x_1^2 + ... + x_n^2 = 1)$ over $\mathbb{F}_p$

Now we analyse the case of $x_1^2 + ... + x_n^2 = 1$ over $\mathbb{F}_p$, so here we have an arbitrary number of variables. By finding expressions for the numbers of solutions we can later on derive larger number theoretical results such as the law of quadratic reciprocity.
Below we use two different methods to count the number of solutions: first we use the previous theory of Gauss sums, where we find that the number of solutions depends only on whether n is even or odd. Then we derive the number of solutions using projective geometry, where we find dependence not only on n but also on the quadratic character of -1 in our field.

5.1 Finding the number of solutions with Gauss sums

We want to find a formula expressed in terms of characters for the number of solutions to the equation $x_1^2 + ... + x_n^2 = 1$ over the field $\mathbb{F}_p$. We recall that when χ is a character of order 2, χ is then uniquely determined and $\chi(\cdot) = \left(\frac{\cdot}{p}\right)$. We can then use the previous result (lemma 2.1.8) that the number of solutions to $x^2 = a$ is given by $N(x^2 = a) = 1 + \chi(a) = 1 + \left(\frac{a}{p}\right)$. We wish to show the following:

Proposition 5.1.1. *Let χ be the character of order 2. For n odd, the number of solutions is given by*

$$N(x_1^2 + ... + x_n^2 = 1) = p^{n-1} + \chi(-1)^{\frac{n-1}{2}} p^{\frac{n-1}{2}}.$$

For n even, the number of solutions is given by

$$N(x_1^2 + ... + x_n^2 = 1) = p^{n-1} - \chi(-1)^{\frac{n}{2}} p^{\frac{n-2}{2}}.$$

Proof. To get an impression of the behaviour of this equation, let us first consider a special case of a small value of n. We will show how to calculate the case $n = 3$:

$$\begin{aligned} N(x_1^2 + x_2^2 + x_3^2 = 1) &= \sum_{a_1+a_2+a_3=1} N(x_1^2 = a_1)N(x_2^2 = a_2)N(x_3^2 = a_3) \\ &= \sum_{a_1+a_2+a_3=1} (1 + \chi(a_1))(1 + \chi(a_2))(1 + \chi(a_3)) \\ &= \sum_{a_1+a_2+a_3=1} \Big(1 + \chi(a_1) + \chi(a_2) + \chi(a_3) + \chi(a_1)\chi(a_2) + \chi(a_1)\chi(a_3) \\ &+ \chi(a_2)\chi(a_3) + \chi(a_1)\chi(a_2)\chi(a_3)\Big). \end{aligned}$$

Here we recognise the expressions for the elementary symmetric polynomials. Recall that the elementary symmetric polynomial in n variables, denoted by $e_k(y_1, ..., y_n)$ for $k = 0, 1, ..., n$, is given by the series

$$e_k(y_1, ..., y_n) = \sum_{1 \leq j_1 < j_2 < ... < j_k \leq n} y_{j_1} \cdot ... \cdot y_{j_k}$$

where $e_0(y_1, ..., y_n) = 1$. We use this to rewrite our Jacobi sums:

$$\begin{aligned} N(x_1^2 + x_2^2 + x_3^2 = 1) &= p^2 + \sum_{a_1,a_2,a_3 \in \mathbb{F}_p} \sum_{1 \leq j \leq 3} \chi(a_j) + \sum_{a_1,a_2,a_3 \in \mathbb{F}_p} \sum_{1 \leq j < k \leq 3} \chi(a_j)\chi(a_k) \\ &+ \sum_{a_1+a_2+a_3=1} \chi(a_1)\chi(a_2)\chi(a_3) \\ &= p^2 + J(\chi, \chi, \chi) + 0 + 0 \\ &= p^2 + J(\chi, \chi, \chi). \end{aligned}$$

That the double sums are zero follows from the fact that $\sum_t \chi(t) = 0$ when we sum over all elements of $\mathbb{F}_p$, so for example $\sum_{a_1 \in \mathbb{F}_p} \chi(a_1) = 0$. Since

$$\sum_{a_1 \in \mathbb{F}_p} \sum_{a_2 \in \mathbb{F}_p} \chi(a_1)\chi(a_2) = \sum_{a_1,a_2 \in \mathbb{F}_p} \chi(a_1 a_2)$$

this is essentially the same as $\sum_{t \in \mathbb{F}_p} \chi(t) = 0,\ t = a_1 a_2$, when the a_i's run through all elements of $\mathbb{F}_p$. We use the same procedure for general n. We have the decomposition

$$\begin{aligned} N(x_1^2 + ... + x_n^2 = 1) &= \sum_{a_1+...+a_n=1} N(x_1^2 = a_1) \cdot ... \cdot N(x_n^2 = a_n) \\ &= \sum_{a_1+...+a_n=1} (1 + \chi(a_1)) \cdot ... \cdot (1 + \chi(a_n)) \\ &= p^{n-1} + \sum_{a_1,...,a_n \in \mathbb{F}_p} \sum_{1 \leq j \leq n} \chi(a_j) + ... \\ &+ \sum_{a_1,...,a_n \in \mathbb{F}_p} \sum_{1 \leq j_1 < j_2 < ... < j_{n-1} \leq n} \chi(a_{j_1}) \cdot ... \cdot \chi(a_{j_{n-1}}) \\ &+ \sum_{a_1+...+a_n=1} \chi(a_1) \cdot ... \cdot \chi(a_n) \\ &= p^{n-1} + 0 + ... + 0 + J(\chi, ..., \chi) \\ &= p^{n-1} + J(\chi, ..., \chi) \end{aligned}$$

where all the double sums are zero by the same reasoning as in the case $n = 3$.

We have to consider the cases of n even and n odd separately. If n is odd, we have $\chi^n = \chi$, and if n is even, $\chi^n = \varepsilon$ (as χ has order 2).

For n odd so $\chi^n \neq \varepsilon$, we can apply theorem 4.0.3, which gives that

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

We also have $g(\lambda)g(\overline{\lambda}) = \lambda(-1)p$ for a character λ by lemma 2.2.5. Since χ here is the unique order 2 character, it is unaffected by complex conjugation, and we have that $g(\overline{\chi}) = g(\chi^{-1}) = g(\chi)$. Then $g(\chi)^2 = \chi(-1)p$, and by inserting into the Jacobi sum above, we get $J(\chi, ..., \chi) = g(\chi)^{n-1} = \chi(-1)^{\frac{n-1}{2}}p^{\frac{n-1}{2}}$.

So for n odd, the number of solutions is given by:

$$N(x_1^2 + ... + x_n^2 = 1) = p^{n-1} + \chi(-1)^{\frac{n-1}{2}}p^{\frac{n-1}{2}}.$$

This proves the first part of the proposition. In the case of n even, we can use corollary 4.0.3.2 of theorem 4.0.3, which states that

$$J(\chi_1, ..., \chi_n) = -\chi_n(-1)J(\chi_1, ..., \chi_{n-1})$$

when $\chi_i \neq \varepsilon$ for all i and $\chi_1 \cdot ... \cdot \chi_n = \varepsilon$.

So in our case, we have $J(\chi, ..., \chi) = -\chi(-1)J(\chi, ..., \chi)$ since χ has order 2, so $\chi \neq \varepsilon$ and $\chi^n = \varepsilon$ (note that in the first Jacobi sum we have n entries, and in the last we have $n-1$ entries). Then, by using the result found for n odd, we get that

$$\begin{aligned} J(\chi, .., \chi) &= -\chi(-1)\frac{g(\chi)^{n-1}}{g(\chi)} \\ &= -\chi(-1)g(\chi)^{n-2} \\ &= -\chi(-1)\chi(-1)^{\frac{n-2}{2}}p^{\frac{n-2}{2}} \\ &= -\chi(-1)^{\frac{n}{2}}p^{\frac{n-2}{2}}. \end{aligned}$$

So in the case where n is even, the number of solutions is given by:

$$N(x_1^2 + ... + x_n^2 = 1) = p^{n-1} - \chi(-1)^{\frac{n}{2}}p^{\frac{n-2}{2}}.$$

This completes the proposition. □

5.2 Finding the number of solutions using projective geometry

Denote by $N_n(a)$ the number of solutions to the equation $x_1^2 + ... + x_n^2 = a$ over $\mathbb{F}_p$, i.e. $N_n(a) = \#\{x_1^2 + ... + x_n^2 = a | (x_1, ..., x_n) \in \mathbb{F}_p^n\}$ and note $\sum\limits_{a \in \mathbb{F}_p} N_n(a) = p^n$. We know that elements in $\mathbb{F}_p$ are either quadratic residues or non-quadratic residues modulo p (below shortened to "squares" and "non-squares" for convenience). Denote by $X(a)$ the set $X_n(a) = \{x_1^2 + ... + x_n^2 = a | (x_1, ..., x_n) \in \mathbb{F}_p^n\}$. Then it holds that

Lemma 5.2.1. *For a a square in $\mathbb{F}_p^*$, there is an isomorphism between $X_n(a)$ and $X_n(1)$.*

Proof. We map $X_n(1)$ to $X_n(a)$ by scaling each x_i by $\frac{1}{\sqrt{a}}$, where we choose one of the two square roots of a (for convenience the positive one). This is then well-defined for $a \in \mathbb{F}_p^*$ a square:

$$\begin{aligned}
\left(\frac{1}{\sqrt{a}}x_1\right)^2 + ... + \left(\frac{1}{\sqrt{a}}x_n\right)^2 &= 1 \\
\Leftrightarrow \frac{1}{a}x_1^2 + ... + \frac{1}{a}x_n^2 &= 1 \\
\Leftrightarrow x_1^2 + ... + x_n^2 &= a \\
&= X_n(a).
\end{aligned}$$

This scaling map has inverse given by multiplication by $\sqrt{a}$ which, by the same type of calculation as above, takes $X_n(a)$ to $X_n(1)$ through scaling each x_i by $\sqrt{a}$ (where again we have chosen a square root). Thus the map is a bijection, and for any a and b that are squares in $\mathbb{F}_p^*$, $X_n(a) \cong X_n(b)$ since they are both isomorphic to $X_n(1)$. □

Lemma 5.2.2. *Analogously, if a and b are both non-squares in $\mathbb{F}_p^*$, we have that $X_n(a) \cong X_n(b)$.*

Proof. If a and b are non-squares, so are their inverses a^{-1} and b^{-1}, and we use that the product of any two non-squares is always a square, i.e. $ab^{-1} = c^2$ for some c in $\mathbb{F}_p^*$. Then by applying the scaling map c to each coordinate x_i, we map $X_n(a)$ to $X_n(b)$:

$$\begin{aligned}
\left(\sqrt{\frac{a}{b}}x_1\right)^2 + ... + \left(\sqrt{\frac{a}{b}}x_n\right)^2 &= a \\
\Leftrightarrow \frac{a}{b}x_1^2 + ... + \frac{a}{b}x_n^2 &= a \\
\Leftrightarrow x_1^2 + ... + x_n^2 &= b \\
&= X_n(b).
\end{aligned}$$

The inverse scaling map $\sqrt{\frac{b}{a}}$ takes $X_n(b)$ to $X_n(a)$, so that $X_n(a) \cong X_n(b)$.

□

Given an equation of the form $x_1^2 + ... + x_n^2 = a$ in $\mathbb{F}_p$, it is useful to consider whether a is a square in $\mathbb{F}_p$ or not in order to ascertain the number of solutions. We will show that the number of solutions $N_n(a)$ only depends on the quadratic character of a in $\mathbb{F}_p$, i.e. on $\left(\frac{a}{p}\right)$. Furthermore, we can derive the following relations between the numbers of solutions:

Lemma 5.2.3. *For $a \in \mathbb{F}_p$ and $N_n(a)$ the number of solutions to $x_1^2 + ... + x_n^2 = a$ over $\mathbb{F}_p$, we have the following relations between the cardinalities of the solution sets:*

$$\sum_{a \in \mathbb{F}_p} N_n(a) = p^n = N_n(0) + \frac{p-1}{2}N_n(square) + \frac{p-1}{2}N_n(non\text{-}square) \tag{5.1}$$

$$N_n(square) = p^{n-1} - N_{n-1}(-1) + N_{n-1}(0) \tag{5.2}$$

$$\frac{N_n(0)-1}{p-1} = N_{n-1}(-1) + \frac{N_{n-1}(0)-1}{p-1} \tag{5.3}$$

Proof. Equation 1 holds since we are summing over the solutions for all $a \in \mathbb{F}_p$, and we can split these naturally into the cases $a = 0$ and a respectively square and non-square in $\mathbb{F}_p$. It follows that there are precisely $\frac{p-1}{2}$ squares and $\frac{p-1}{2}$ non-squares in $\mathbb{F}_p$ by considering the group homomorphism $f : \mathbb{F}_p^* \to \mathbb{F}_p^*$ given by $f(a) = a^2$. The kernel of this map has order 2, and since $\mathbb{F}_p^*$ has $p - 1$ elements, there are $\frac{p-1}{2}$ squares and thus $\frac{p-1}{2}$ non-squares.

To derive equation 2, we apply stereographic projection. Stereographic projection is given by a map that projects a sphere onto a plane. This map is smooth, bijective and defined everywhere, save the point from which we project. To understand equation 2, we first look at a concrete small n, $n = 3$. Let $X = \{x_1^2 + x_2^2 + x_3^2 = 1 | (x_1, x_2, x_3) \in \mathbb{F}_p^3\}$. Then $Q_0 = (-1, 0, 0) \in X$, and for s and t free variables, points of the form $P = (0, s, t)$ defines the plane where $x_1 = 0$. Call this plane Y. Then we find the line L through Q_0 and P: for $0 \leq \alpha \leq 1$, L is given by:

$$(1 - \alpha)(-1, 0, 0) + \alpha(0, s, t) = (\alpha - 1, \alpha s, \alpha t).$$

We find the intersection between X and L:

$$\begin{aligned}(\alpha - 1)^2 + (\alpha s)^2 + (\alpha t)^2 &= 1\\ \Leftrightarrow (1 + s^2 + t^2)\alpha^2 - 2\alpha &= 0\\ \Leftrightarrow \alpha = 0 \quad \text{or} \quad \alpha = \frac{2}{1 + s^2 + t^2}&.\end{aligned}$$

Since $\alpha = 0$ corresponds to Q_0, we can discard this solution, so we get the point

$$\left(\frac{2}{1 + s^2 + t^2} - 1, \frac{2s}{1 + s^2 + t^2}, \frac{2t}{1 + s^2 + t^2}\right) \in X.$$

This map is well-defined if we exclude the pairs (s, t) in Y such that $1 + s^2 + t^2 = 0$. To go the other way and find the point in Y, we construct the inverse of the above map:

$$(1 - \alpha)(-1, 0, 0) + \alpha(x_1, x_2, x_3) = (\alpha - 1 + \alpha x_1, \alpha x_2, \alpha x_3).$$

This line hits the plane for $\alpha - 1 + \alpha x_1 = 0 \Leftrightarrow \alpha = \frac{1}{1+x_1}$. So we get the point in the plane

$$\left(0, \frac{x_2}{1 + x_1}, \frac{x_3}{1 + x_1}\right).$$

Again, this map is well-defined when we exclude all points (x_1, x_2, x_3) such that $x_1 = -1$. By use of the isomorphism $Y = \{(0, s, t) \in \mathbb{F}_p^3\} \cong \mathbb{F}_p \times \mathbb{F}_p$, we have a bijection between the sets $\mathbb{F}_p \times \mathbb{F}_p \backslash \{(s, t) | s^2 + t^2 = -1\}$ and $X \backslash \{(x_1, x_2, x_3) | x_1 = -1\}$. When we count the points in each of these sets, we arrive at the identity

$$p^2 - N_2(-1) = N_3(\text{square}) - N_2(0).$$

This gives insight into equation 2 for $n = 3$. We can use the same procedure for general n, and we find the map

$$\begin{aligned}f : H\backslash\{(s_1, ..., s_{n-1}) | s_1^2 + ... + s_{n-1}^2 = -1\} &\to X\backslash\{(x_1, ..., x_n) | x_1 = -1\}\\ f(0, s_1, ..., s_{n-1}) = \left(\frac{2}{1 + s_1^2 + ... + s_{n-1}^2} - 1, \right.&\left.\frac{2s_1}{1 + s_1^2 + ... + s_{n-1}^2}, ..., \frac{2s_{n-1}}{1 + s_1^2 + ... + s_{n-1}^2}\right)\end{aligned}$$

with inverse

$$\begin{aligned} f^{-1}: X\backslash\{(x_1,...,x_n)|x_1=-1\} &\to H\backslash\{(s_1,...,s_{n-1})|s_1^2+...+s_{n-1}^2=-1\} \\ (x_1,...,x_n) &\mapsto \left(0,\frac{x_2}{1+x_1},...,\frac{x_n}{1+x_1}\right) \end{aligned}$$

where $X=\{x_1^2+...+x_n^2=1|(x_1,...,x_n)\in\mathbb{F}_p^n\}$ and H is the hyperplane corresponding to $x_1=0$. Again, as $H=\{(0,s_1,...,s_{n-1})\in\mathbb{F}_p^n\}\cong\mathbb{F}_p^{n-1}$, then by the method of counting points in these sets we find the identity

$$p^{n-1}-N_{n-1}(-1)=N_{n-1}(square)-N_{n-1}(0)$$

which in the case $n+1$ directly gives equation 2.

For equation 3, we see that it is equivalent to the expression

$$N_n(0)=(p-1)N_{n-1}(-1)+N_{n-1}(0).$$

This expression holds since we can split an equation of the form $x_1^2+...+x_n^2=0$ into the cases $x_n=0$ and $x_n\neq 0$. When counting solutions to these cases we get $N_{n-1}(0)$ and $(p-1)N_{n-1}(-1)$. The latter follows since there are $p-1$ choices for x_n, and we can divide the whole equation by $x_n\neq 0$ and rearrange the equation. Combining these two cases gives equation 3. □

We would like to find a recursive relationship between the equations of lemma 5.2.3. First we consider the number of solutions in the case $n=1$: $N_1(square)=2$, corresponding to the solutions to $x_1^2=1$ where x_1 is a square in $\mathbb{F}_p$. Similarly we have that $N_1(non-square)=0$, corresponding to the case $x_1^2=1$ for x_1 not a square in $\mathbb{F}_p$. Finally, $N_1(0)=1$, corresponding to $x_1^2=0$. From these we could, in theory, calculate all values of $N_n(0), N_n(square)$ and $N_n(non-square)$ successively, however from a certain step we can derive recursive formulas. For simplicity, we consider the cases -1 square and -1 non-square separately. By use of the previous we find the following results:

Theorem 5.2.4. *When -1 is a square in $\mathbb{F}_p$, we have the following relationships between the number of solutions for $n\geq 4$: in the case where n is even:*

$$\begin{aligned} \text{Case 1) } N_n(0) &= p^{n-1}+p^{\frac{n}{2}}-p^{\frac{n-2}{2}}; \\ N_n(1) &= N_n(-1)=N_n(square)=p^{\frac{n-2}{2}}\left(p^{\frac{n}{2}}-1\right); \\ N_n(non-square) &= p^{n-1}-p^{\frac{n-2}{2}}. \end{aligned}$$

In the case where n is odd:

$$\begin{aligned} \text{Case 2) } N_n(0) &= p^{n-1}; \\ N_n(1) &= N_n(-1)=N_n(square)=p^{n-1}+p^{\frac{n-1}{2}}; \\ N_n(non-square) &= p^{n-1}-p^{\frac{n-1}{2}}. \end{aligned}$$

Proof. We prove each case separately. We start by verifying the identities for $n = 4$. We do this by applying the stated formulas (we skip the details for calculating N_2 and N_3 since they are easily found by knowing the values of N_1) and find:

$$\begin{aligned}
N_4(0) &= (p-1)N_3(-1) + N_3(0)\\
&= (p-1)N_3(square) + N_3(0)\\
&= (p-1)(p^2+p) + p^2\\
&= p^3 + p^2 - p.\\
N_4(square) &= p^3 - N_3(-1) + N_3(0)\\
&= p^3 - N_3(square) + N_3(0)\\
&= p^3 - p^2 - p + p^2\\
&= p^3 - p.\\
(p-1)N_4(non-square) &= 2p^4 - 2N_4(0) - (p-1)N_4(square)\\
&= 2p^4 - 2(p^3+p^2-p) - (p-1)(p^3-p)\\
\Leftrightarrow N_4(non-square) &= p^3 - p
\end{aligned}$$

which verifies the start of the proof. We now assume case 1 holds, so that n is even, and show that this implies case 2 for $n+1$, which is odd. First:

$$\begin{aligned}
N_{n+1}(0) &= (p-1)N_n(-1) + N_n(0)\\
&= (p-1)p^{\frac{n-2}{2}}\left(p^{\frac{n}{2}} - 1\right)\\
&= p^n.
\end{aligned}$$

Secondly:

$$\begin{aligned}
N_{n+1}(square) &= p^n - N_n(-1) + N_n(0)\\
&= p^n - p^{\frac{n-2}{2}}\left(p^{\frac{n}{2}} - 1\right) + p^{n-1} + p^{\frac{n}{2}} - p^{\frac{n-2}{2}}\\
&= p^n + p^{\frac{n}{2}}.
\end{aligned}$$

And finally:

$$\begin{aligned}
(p-1)N_{n+1}(non-square) &= 2p^{n+1} - 2N_{n+1}(0) - (p-1)N_{n+1}(square)\\
&= 2p^{n+1} - 2p^n - (p-1)\left(p^n + p^{\frac{n}{2}}\right)
\end{aligned}$$

which is equivalent to:

$$\begin{aligned}
N_{n+1}(non-square) &= \frac{2p^{n+1} - 2p^n - (p-1)\left(p^n + p^{\frac{n}{2}}\right)}{p-1}\\
&= p^n - p^{\frac{n}{2}}.
\end{aligned}$$

These are the correct identities. Now we assume case 2, so that n is odd, and show that this implies case 1 for $n+1$, which is even. First we find:

$$\begin{aligned}
N_{n+1}(0) &= (p-1)N_n(-1) + N_n(0)\\
&= (p-1)\left(p^{n-1} + p^{\frac{n-1}{2}}\right) + p^{n-1}\\
&= p^n + p^{\frac{n+1}{2}} - p^{\frac{n-1}{2}}.
\end{aligned}$$

Secondly:

$$\begin{aligned}N_{n+1}(square) &= p^n - N_n(-1) + N_n(0)\\ &= p^n - \left(p^{n-1} + p^{\frac{n-1}{2}}\right) + p^{n-1}\\ &= p^n - p^{\frac{n-1}{2}}.\end{aligned}$$

And finally:

$$\begin{aligned}(p-1)N_{n+1}(non-square) &= 2p^{n+1} - 2N_{n+1}(0) - (p-1)N_{n+1}(square)\\ &= 2p^{n+1} - 2\left(p^n + p^{\frac{n+1}{2}} - p^{\frac{n-1}{2}}\right) - (p-1)\left(p^n - p^{\frac{n-1}{2}}\right)\end{aligned}$$

which is equivalent to:

$$\begin{aligned}N_{n+1}(non-square) &= \frac{2p^{n+1} - 2\left(p^n + p^{\frac{n+1}{2}} - p^{\frac{n-1}{2}}\right) - (p-1)\left(p^n - p^{\frac{n-1}{2}}\right)}{p-1}\\ &= p^n - p^{\frac{n-1}{2}}.\end{aligned}$$

These are the correct identities, and this completes the proof in the case where -1 is a square. □

Theorem 5.2.5. *When -1 is non-square in $\mathbb{F}_p$, we have the following relationships between the number of solutions for $n \geq 4$: in the case where n is even:*

$$\begin{aligned}\text{Case 3) } N_n(0) &= p^{n-1} + (-1)^{\frac{n}{2}}\left(p^{\frac{n}{2}} - p^{\frac{n-2}{2}}\right);\\ N_n(1) &= N_n(square) = p^{n-1} - (-1)^{\frac{n}{2}}p^{\frac{n-2}{2}};\\ N_n(-1) &= N_n(non-square) = p^{\frac{n-2}{2}}\left(p^{\frac{n}{2}} - (-1)^{\frac{n}{2}}\right).\end{aligned}$$

In the case when n is odd:

$$\begin{aligned}\text{Case 4) } N_n(0) &= p^{n-1};\\ N_n(1) &= N_n(square) = p^{n-1} + (-1)^{\frac{n-1}{2}}p^{\frac{n-1}{2}};\\ N_n(-1) &= N_n(non-square) = p^{\frac{n-1}{2}}\left(p^{\frac{n-1}{2}} - (-1)^{\frac{n-1}{2}}\right).\end{aligned}$$

Proof. Again we use induction. First we verify the start for $n = 4$ (again this is done directly by calculation of $n = 2, 3$, but we will not show all steps here):

$$\begin{aligned}N_4(0) &= (p-1)N_3(-1) + N_3(0)\\ &= (p-1)N_3(non-square) + N_3(0)\\ &= (p-1)p(p+1) + p^2\\ &= p(p^2+p-1).\\ N_4(square) &= p^3 - N_3(-1) + N_3(0)\\ &= p^3 - N_3(non-square) + N_3(0)\\ &= p^3 - p(p+1) + p^2\\ &= p^3 - p.\\ (p-1)N_4(non-square) &= 2p^4 - 2N_4(0) - (p-1)N_4(square)\\ &= 2p^4 - 2p(p^2+p-1) - (p-1)(p^3-p)\\ \Leftrightarrow N_4(non-square) &= p(p^2-1).\end{aligned}$$

We see that the expressions hold for the induction start. We now assume that case 3 holds for n, which is even, and show that this implies case 4 for $n+1$, which is odd:

$$\begin{aligned} N_{n+1}(0) &= (p-1)N_n(-1) + N_n(0) \\ &= (p-1)p^{\frac{n-2}{2}}\left(p^{\frac{n}{2}} - (-1)^{\frac{n}{2}}\right) + p^{n-1} + (-1)^{\frac{n}{2}}\left(p^{\frac{n}{2}} - p^{\frac{n-2}{2}}\right) \\ &= p^n. \end{aligned}$$

Secondly:

$$\begin{aligned} N_{n+1}(square) &= p^n - N_n(-1) + N_n(0) \\ &= p^n - p^{\frac{n-2}{2}}\left(p^{\frac{n}{2}} - (-1)^{\frac{n}{2}}\right) + p^{n-1} + (-1)^{\frac{n}{2}}\left(p^{\frac{n}{2}} - p^{\frac{n-2}{2}}\right) \\ &= p^n + (-1)^{\frac{n}{2}}p^{\frac{n}{2}}. \end{aligned}$$

And finally:

$$\begin{aligned} (p-1)N_{n+1}(non-square) &= 2p^{n+1} - 2N_{n+1}(0) - (p-1)N_{n+1}(square) \\ &= 2p^{n+1} - 2p^n - (p-1)\left(p^n + (-1)^{\frac{n}{2}}p^{\frac{n}{2}}\right) \end{aligned}$$

which is equivalent to:

$$\begin{aligned} N_{n+1}(non-square) &= \frac{2p^{n+1} - 2p^n - (p-1)\left(p^n + (-1)^{\frac{n}{2}}p^{\frac{n}{2}}\right)}{p-1} \\ &= p^n - (-1)^{\frac{n}{2}}p^{\frac{n}{2}}. \end{aligned}$$

These have the correct forms. Lastly we assume that case 4 holds for n, which is odd, and show that this implies case 3 for $n+1$, which is even:

$$\begin{aligned} N_{n+1}(0) &= (p-1)N_n(-1) + N_n(0) \\ &= (p-1)p^{\frac{n-1}{2}}\left(p^{\frac{n-1}{2}} - (-1)^{\frac{n-1}{2}}\right) + p^{n-1} \\ &= p^n + (-1)^{\frac{n-1}{2}}\left(p^{\frac{n-1}{2}} - p^{\frac{n+1}{2}}\right) \end{aligned}$$

which holds when noting that we must have:

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

Next we have that:

$$\begin{aligned} N_{n+1}(square) &= p^n - N_n(-1) + N_n(0) \\ &= p^n - p^{\frac{n-1}{2}}\left(p^{\frac{n-1}{2}} - (-1)^{\frac{n-1}{2}}\right) + p^{n-1} \\ &= p^n + (-1)^{\frac{n-1}{2}}p^{\frac{n-1}{2}} \end{aligned}$$

which again holds when we note:

$$p^n + (-1)^{\frac{n-1}{2}}p^{\frac{n-1}{2}} = p^n - (-1)^{\frac{n+1}{2}}p^{\frac{n-1}{2}}.$$

Finally:

$$\begin{aligned}(p-1)N_{n+1}(non-square) &= 2p^{n+1}-2N_{n+1}(0)-(p-1)N_{n+1}(square)\\ &= 2p^{n+1}-2\left(p^n+(-1)^{\frac{n+1}{2}}\left(p^{\frac{n+1}{2}}-p^{\frac{n-1}{2}}\right)\right)\\ &- (p-1)\left(p^n-(-1)^{\frac{n+1}{2}}p^{\frac{n-1}{2}}\right)\end{aligned}$$

which is equivalent to:

$$\begin{aligned}N_{n+1}(non-square) &= \frac{2p^{n+1}-2\left(p^n+(-1)^{\frac{n+1}{2}}\left(p^{\frac{n+1}{2}}-p^{\frac{n-1}{2}}\right)\right)}{p-1}\\ &- \frac{(p-1)\left(p^n-(-1)^{\frac{n+1}{2}}p^{\frac{n-1}{2}}\right)}{p-1}\\ &= p^n-(-1)^{\frac{n+1}{2}}p^{\frac{n-1}{2}}.\end{aligned}$$

So we arrive at all the correct forms which completes the proof. □

All of these, both in the case of -1 square and non-square in $\mathbb{F}_p$, are consistent with what we found using Jacobi sums in proposition 5.1.1.

Deriving the quadratic character of 2 in $\mathbb{F}_p$

In the following we give a description of the quadratic character of 2 in a field $\mathbb{F}_p$. By using group theory, we wish to show the following theorem:

Theorem 6.0.1. *Let χ be the Legendre symbol over our field $\mathbb{F}_p$. Then $\chi(2) = 1$ for $p \equiv \pm 1 \mod 8$, and $\chi(2) = -1$ for $p \equiv 3 \mod 8$ or $p \equiv 5 \mod 8$.*

Proof. In the previous chapter we have shown that the number of solutions to $x^2 + y^2 = 1$ over $\mathbb{F}_p$ is equal to $p \pm 1$, with $p - 1$ when -1 is a square and $p + 1$ when -1 is non-square.

In the following, let G be a finite (non-commutative) group of order 8. We recall that if we let a finite group act on a set, the orbits of the group action give a partition of this set. Hence if we let G act on the set $S = \{x^2 + y^2 = 1 | (x, y) \in \mathbb{F}_p^2\}$, we then get S as a disjoint union of the orbits of S under G.

We define the free orbits of G as the ones of order 8 (i.e. of the same order as the group itself). This also gives us the following identity in the case where -1 is a square in $\mathbb{F}_p$:

$$\begin{aligned} \#\{x^2 + y^2 = 1 | (x, y) \in \mathbb{F}_p^2\} &= p - 1 \\ &= \sum_{orbits\ of\ G\ on\ S} (size\ of\ orbit) \\ &\equiv \sum_{non-free\ orbits\ of\ G\ on\ S} (size\ of\ orbit) \mod 8 \end{aligned}$$

as we can split the sum over all orbits into two, one over the free orbits and one over the non-free orbits, and then mod out by 8. Similarly, for -1 non-square in $\mathbb{F}_p$, we have:

$$\begin{aligned} p + 1 &= \sum_{orbits\ of\ G\ on\ S} (size\ of\ orbit) \\ &\equiv \sum_{non-free\ orbits\ of\ G\ on\ S} (size\ of\ orbit) \mod 8. \end{aligned}$$

For finite groups, the order of any orbit must be a divisor of the group order, so any orbit must have size $1, 2, 4$ or 8. We recall here the result that $|O_x| = |G|/|G_x|$, where O_x denotes the orbit of x and G_x denotes the stabilizer of x.

Given a pair $(x, y) \in \mathbb{F}_p \times \mathbb{F}_p$ satisfying $x^2 + y^2 = 1$, the orbit of x, respectively y, is non-free if there exists a non-trivial stabilizer, i.e. if there is some $g \neq 1 \in G$ such that $g(x, y) = (x, y)$. Given the pair $(x, y) \in \mathbb{F}_p^2$, the possible group actions are given by:

$$(x, y), (-x, -y), (-y, x), (y, -x), (-y, -x), (y, x), (x, -y)$$

of which 6 are seen to be non-trivial. By inspection this reduces to considering the four cases $x = y, x = -x, y = -y$ and $x = -y$. We count all elements satisfying one of these, making sure there is no overlap: the cases

$$\begin{aligned}
1)\ x &= -y, x = -x \\
2)\ x &= -y, y = -y \\
3)\ x &= -y, x = y \\
4)\ x &= -x, y = -y \\
5)\ x &= -x, x = y \\
6)\ y &= -y, x = y
\end{aligned}$$

all lead to the contradiction $x = y = 0$ so that $x^2 + y^2 = 1$ fails. Hence no pair $(x, y) \in \mathbb{F}_p^2$ such that that $x^2 + y^2 = 1$ will fulfil more than one of the equalities in the list.

The cases $x = -x$ and $y = -y$ each correspond to 2 solutions, by the condition $x^2 + y^2 = 1$. The condition $x^2 + y^2 = 1$ also implies that the cases $x = y$ and $x = -y$ have the same number of solutions, and we use the previous fact (lemma 2.1.8) that

$$N(x^2 = a) = 1 + \chi(a)$$

where χ is the multiplicative character of order 2, the Legendre symbol. Since $\mathbb{F}_p$ is a field, we have a bijection between the sets $\{x^2 = \frac{1}{2} | x \in \mathbb{F}_p\}$ and $\{x^2 = 2 | x \in \mathbb{F}_p\}$, which follows from $x = y$, so that $2x^2 = 1$. So for the cases $x = y$ and $x = -y$, we get $1 + \chi(2)$ solutions both times. From the above we see that for -1 a square in $\mathbb{F}_p$:

$$\begin{aligned}
p - 1 &\equiv 2 + 2 + 1 + \chi(2) + 1 + \chi(2) \mod 8 \\
&\equiv 6 + 2\chi(2) \mod 8.
\end{aligned}$$

Hence $\chi(2) = 1$ for $p \equiv \pm 1 \mod 8$, and $\chi(2) = -1$ if $p \equiv 3 \mod 8$ or $p \equiv 5 \mod 8$. Analogously, for -1 non-square in $\mathbb{F}_p$:

$$p + 1 \equiv 6 + 2\chi(2) \mod 8.$$

Hence we have $\chi(2) = 1$ for $p \equiv \pm 1 \mod 8$, and $\chi(2) = -1$ if $p \equiv 3 \mod 8$ or $p \equiv 5 \mod 8$. This completes the proof. □

Example 6.0.2.

Let us see an example of how to determine the quadratic character of 2 in a given finite field. Let $p = 5$, then -1 is square in $\mathbb{F}_5$. Then the theorem gives directly that $\chi(2) = -1$, however we can also see this just from the group theory observations:

$$\begin{aligned}
p - 1 &= 5 - 1 = 4 \\
&\equiv 6 + 2\chi(2) \mod 8
\end{aligned}$$

so we can see directly that $\chi(2) = \left(\frac{2}{5}\right) = -1$. If $p = 7$ so -1 is non-square in $\mathbb{F}_7$, we have

$$\begin{aligned} p+1 &= 7+1 = 8 \\ &\equiv 6 + 2\chi(2) \mod 8. \end{aligned}$$

Hence $\chi(2) = \left(\frac{2}{7}\right) = 1$ in this case.

6.1 The quadratic character of -1 in $\mathbb{F}_p$

From the above, we can also derive the quadratic character of -1 in $\mathbb{F}_p$:

Proposition 6.1.1.

$$\chi(-1) \equiv p \mod 4.$$

Proof. This is equivalent to

$$p - \chi(-1) \equiv 0 \mod 4$$

which follows as we found that $p \pm 1 \equiv 6 + 2\chi(2) \mod 8$ by considering the size of the non-free orbits. We found this result by reducing to the cases:

a) $x = -x$ and $y = -y$, which each has 2 solutions, giving 4 solutions in total;

b) $x = y$ and $x = -y$, which each has $1 + \chi(2)$ solutions, giving either 0 or 4 solutions in total. This means that the non-free orbits all have size divisible by 4, hence

$$\chi(-1) \equiv p \mod 4.$$

□

Deriving the law of quadratic reciprocity

Based on our previous analysis of the equation $x_1^2 + ... + x_n^2 = 1$ over $\mathbb{F}_p$, we can derive the quadratic character of odd primes modulo p, giving us results about quadratic reciprocity. We now consider the case of $n = q$, where q is an odd prime, $q \neq p$. We will prove the following version of the law of quadratic reciprocity:

Theorem 7.0.1. *For p and q odd primes, $p \neq q$, and $\chi(\cdot) = \left(\frac{\cdot}{p}\right)$, we have the relation*

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

Proof. In the following, we work with the cyclic group G of order q, acting on the finite set $S = \{x_1^2 + ... + x_q^2 = 1 | (x_1, ..., x_q) \in \mathbb{F}_p^q\}$. G acts on S by cyclically permuting the variables; if $g \in G$ is a generator, the action is given by $g(x_1, ..., x_q) = (x_q, x_1, ..., x_{q-1})$, which has order q. Since the orbits must have size dividing q, all orbits necessarily have size 1 or q since q is prime. By use of Gauss sums, we showed in proposition 5.1.1 that for an odd number of variables, the number of solutions is given by the expression

$$N(x_1^2 + ... + x_q^2 = 1) = p^{q-1} + \chi(-1)^{\frac{q-1}{2}} p^{\frac{q-1}{2}}$$

where χ denotes the Legendre symbol. As in the case of 2, we have that

$$\begin{aligned} p^{q-1} + \chi(-1)^{\frac{q-1}{2}} p^{\frac{q-1}{2}} &= \#\{x_1^2 + ... + x_q^2 = 1 | (x_1, ..., x_q) \in \mathbb{F}_p^q\} \\ &= \sum_{orbits\ of\ G\ on\ S} (size\ of\ orbit) \\ &\equiv \sum_{non-free\ orbits\ of\ G\ on\ S} (size\ of\ orbit) \mod q. \end{aligned}$$

Since the free orbits are the ones of order q, and q is prime, we are left with the orbits of order 1, belonging to the case where $x_1 = x_2 = ... = x_q = x$ so that $x_1^2 + ... + x_q^2 = qx^2$. Since $\mathbb{F}_p$ is a field, we can again construct a bijection between the sets $\{x^2 = \frac{1}{q} | x \in \mathbb{F}_p\}$ and $\{x^2 = q | x \in \mathbb{F}_p\}$, so that these equations have the same numbers of solutions over $\mathbb{F}_p$. By lemma 2.1.8 we have

$$N(x^2 = q) = 1 + \chi(q).$$

By the above, we have that

$$\begin{aligned} p^{q-1} + \chi(-1)^{\frac{q-1}{2}} p^{\frac{q-1}{2}} &\equiv 1 + \chi(q) \mod q \\ \Leftrightarrow 1 + \chi(-1)^{\frac{q-1}{2}} p^{\frac{q-1}{2}} &\equiv 1 + \chi(q) \mod q \\ \Leftrightarrow \chi(-1)^{\frac{q-1}{2}} p^{\frac{q-1}{2}} &\equiv \chi(q) \mod q \end{aligned}$$

where the second line follows by Fermat's little theorem, as $p \not| q$. Since $p^{\frac{q-1}{2}} = \left(\frac{p}{q}\right)$ and by definition, $\chi(q) = \left(\frac{q}{p}\right)$, we have

$$\begin{aligned} \chi(-1)^{\frac{q-1}{2}} \left(\frac{p}{q}\right) &\equiv \left(\frac{q}{p}\right) \mod q \\ \Leftrightarrow \chi(-1)^{\frac{q-1}{2}} &\equiv \left(\frac{p}{q}\right)\left(\frac{q}{p}\right) \mod q \\ \Leftrightarrow (-1)^{\frac{p-1}{2}\frac{q-1}{2}} &\equiv \left(\frac{p}{q}\right)\left(\frac{q}{p}\right) \mod q \end{aligned}$$

since by definition of the Legendre symbol, $\left(\frac{p}{q}\right)^{-1} = \left(\frac{p}{q}\right)$ and $\chi(-1) = (-1)^{\frac{p-1}{2}}$. We note that we can disregard having to work $\mod q$, since for $\pm 1 \equiv \pm 1 \mod n$ and $n > 2$ (so that $-1 \not\equiv 1 \mod n$), the left and right side are also identical over $\mathbb{Z}$. This precisely gives us the law of quadratic reciprocity. □

Example 7.0.2.

Let us see an example of how one can calculate the quadratic character of an odd prime q in $\mathbb{F}_p$. Let $q = 3$ and $p = 5$, so that -1 is a square in $\mathbb{F}_p$. By the group theoretical results above, we have

$$\begin{aligned} 1 + \chi(3) &\equiv 5^{3-1} + \chi(-1)^{\frac{3-1}{2}} 5^{\frac{3-1}{2}} \\ &= 5^2 + 5 \\ &\equiv 0 \mod 5 \end{aligned}$$

from which we see that $\chi(3) = \left(\frac{3}{5}\right) = -1$. If $p = 7$, so that -1 is non-square, we find that

$$\begin{aligned} 1 + \chi(3) &\equiv 7^{3-1} + \chi(-1)^{\frac{3-1}{2}} 7^{\frac{3-1}{2}} \\ &= 7^2 - 7 \\ &\equiv 2 \mod 5 \end{aligned}$$

so that $\chi(3) = \left(\frac{3}{7}\right) = 1$.

The Hasse-Davenport Relation

We now return to the study of Gauss sums. Let $\mathbb{F}$ be a finite field with q elements, q not necessarily prime, and let $\mathbb{E}$ be a field extension of $\mathbb{F}$ of degree s. Let $\chi \neq \varepsilon$ be a character on $\mathbb{F}$. Then we wish to define the extended character χ' on $\mathbb{E}$:

Definition 8.0.1. *For finite fields $\mathbb{F}$ and $\mathbb{E}$ such that $\mathbb{F} \subset \mathbb{E}$ and χ is a character on $\mathbb{F}$, we define the extension of χ to $\mathbb{E}$, denoted by χ', as*

$$\chi'(\alpha) = (\chi \circ N_{\mathbb{E}/\mathbb{F}})(\alpha) = \chi(N_{\mathbb{E}/\mathbb{F}}(\alpha))$$

where $N_{\mathbb{E}/\mathbb{F}}$ is the relative norm. By this definition χ' is a multiplicative character on $\mathbb{E}$.

For g a Gauss sum as previously defined in chapter 2, we wish to find the relation between $g(\chi)$ and $g(\chi')$. This will be given by the Hasse-Davenport relation.
To do this, we first need to recall certain algebraic results, such as the properties of norm and trace. We need the following results:

Proposition 8.0.2. *Let $F_d(x)$ be the product of the monic irreducible polynomials in $\mathbb{Z}/p\mathbb{Z}[x]$ of degree d. Then we have that*

$$x^{p^n} - x = \prod_{d|n} F_d(x).$$

Proof. First note that this product is finite, since it has p^{d+1} terms. Then note that for a non-constant polynomial f, then if $f(x)|x^{p^n} - x$, then $f(x)^2 \not| x^{p^n} - x$, since if $x^{p^n} - x = f(x)^2 g(x)$ then by differentiation

$$-1 = 2f(x)f'(x)g(x) + f(x)^2 g'(x).$$

This would imply $f(x)| - 1$, which is a contradiction. What we must show now is that for f a monic irreducible polynomial of degree d, then $f(x)|x^{p^n} - x$ if and only if $d|n$. Let $\mathbb{K} = \mathbb{Z}/p\mathbb{Z}(\alpha)$ where $f(\alpha) = 0$. Then $[\mathbb{K} : \mathbb{Z}/p\mathbb{Z}] = d$ and so $\mathbb{K}$ has p^d elements, and $x^{p^d} - x = 0$ for $x \in \mathbb{K}$.
Now assume that $x^{p^n} - x = f(x)g(x)$. Then $\alpha^{p^n} = \alpha$. If we take an element in $\mathbb{K}$, we know it has the form $a_1\alpha^{d-1} + a_2\alpha^{d-2} + ... + a_d$, and then we have

$$\begin{aligned} (a_1\alpha^{d-1} + ... + a_d)^{p^n} &= a_1(\alpha^{p^n})^{d-1} + ... + a_d \\ &= a_1\alpha^{d-1} + ... + a_d \end{aligned}$$

since $\mathbb{K}$ has characteristic p. Hence $x^{p^n} - x = 0$ for $x \in \mathbb{K}$. We know that in fields, for $a \in \mathbb{N}$, $a^l - 1|a^m - 1$ if and only if $l|m$. Similarly, $x^l - 1|x^m - 1$ in $\mathbb{F}[x]$ if and only if $l|m$.

This means that since $x^{p^d} - x | x^{p^n} - x$, d must be a divisor of n. On the other hand, if $d|n$, then since $\alpha^{p^d} = \alpha$ and $f(x)$ is the monic irreducible polynomium for α, we have that $f(x)|x^{p^d} - x$. Since $d|n$, $x^{p^d} - x|x^{p^n} - x$, hence $f(x)|x^{p^n} - x$. □

Definition 8.0.3. *Let $\mathbb{F}$ be a finite field with q elements, q not necessarily prime, and let $\mathbb{E}$ be a field extension of $\mathbb{F}$ of degree s, so that $\mathbb{E}$ has q^s elements. For α in $\mathbb{E}$, we define, respectively, the trace and norm of α from $\mathbb{E}$ to $\mathbb{F}$ by*

$$\begin{aligned} Tr_{\mathbb{E}/\mathbb{F}} &= \alpha + \alpha^q + ... + \alpha^{q^{s-1}} \\ N_{\mathbb{E}/\mathbb{F}} &= \alpha \cdot \alpha^q \cdot ... \cdot \alpha^{q^{s-1}}. \end{aligned}$$

We also need some basic results involving the properties of the relative norm and -trace:

Proposition 8.0.4. *Let $\mathbb{F}, \mathbb{E}, \mathbb{K}$ be finite fields such that $\mathbb{F} \subset \mathbb{E} \subset \mathbb{K}$. Let $d = [\mathbb{E} : \mathbb{F}], m = [\mathbb{K} : \mathbb{E}]$ and $n = [\mathbb{K} : \mathbb{F}]$. Let $\mathbb{F}$ have q elements, and let $\alpha \in \mathbb{K}$. Then it holds that*

$$Tr_{\mathbb{K}/\mathbb{F}}(\alpha) = Tr_{\mathbb{E}/\mathbb{F}}(Tr_{\mathbb{K}/\mathbb{E}}(\alpha)).$$

Proof. We know from the extension theorems that $n = dm$. Since the number of elements in $\mathbb{E}$ is $q_1 = q^d$, we have the traces

$$\begin{aligned} Tr_{\mathbb{K}/\mathbb{E}}(\alpha) &= \alpha + ... + \alpha^{q_1^{m-1}} \\ Tr_{\mathbb{E}/\mathbb{F}}(Tr_{\mathbb{K}/\mathbb{E}}(\alpha)) &= \sum_{i=0}^{d-1} Tr_{\mathbb{K}/\mathbb{E}}(\alpha)^{q^i} \\ &= \sum_{i=0}^{d-1} \sum_{j=0}^{m-1} \alpha^{{q_1}^j q^i} \\ &= \sum_{i=0}^{d-1} \sum_{j=0}^{m-1} \alpha^{q^{dj+i}} \\ &= \sum_{k=0}^{n-1} \alpha^{q^k} \\ &= Tr_{\mathbb{K}/\mathbb{F}}(\alpha). \end{aligned}$$

This follows from the fact that by letting j run from 0 to $m-1$ and i from 0 to $d-1$, the power $dj + i$ runs from 0 to $d(m-1) + (d-1) = dm - 1 = n - 1$. □

Proposition 8.0.5. *Let $\mathbb{K}$ and $\mathbb{F}$ be finite fields such that $\mathbb{F} \subset \mathbb{K}$ and $n = [\mathbb{K} : \mathbb{F}]$. Let $\mathbb{F}$ be the field with q elements, and let α be an element of $\mathbb{K}$. Let $f(x)$ be the minimal polynomial for α over $\mathbb{F}$, and let $\mathbb{E} = \mathbb{F}(\alpha)$. Then we know that $[\mathbb{E} : \mathbb{F}] = d$ for $d = \deg(f)$. Write f as*

$$f(x) = x^d - a_1 x^{d-1} + ... + (-1)^d a_d.$$

Then the following hold:

a) $f(x) = (x - \alpha)(x - \alpha^q) \cdot ... \cdot (x - \alpha^{q^{d-1}})$;

b) $Tr_{\mathbb{K}/\mathbb{F}}(\alpha) = \frac{n}{d}a_1$;

c) $N_{\mathbb{K}/\mathbb{F}}(\alpha) = a_d^{\frac{n}{d}}$.

Proof. a) Since $\mathbb{F}$ is of characteristic q, we know the coefficients of f satisfy $a_i^q = a_i$, so we have

$$f(\alpha^q) = f(\alpha)^q = 0$$

so that α^q is another root of f. Since it also holds that

$$f(\alpha^{q^2}) = f(\alpha^q)^q = 0,$$

α^{q^2} is also a root. In this manner we find that the roots of f are $\alpha, ..., \alpha^{q^{d-1}}$. To prove a), we need to show that all these roots are distinct. Assume that $\alpha^{q^i} = \alpha^{q^j}$ for $0 \leq i \leq j < d$ and let $k = j - i$. Now we show that $k = 0$. We have

$$\begin{aligned} \alpha^{q^i} = \alpha^{q^j} = \alpha^{q^{j-i+i}} &= (\alpha^{q^k})^{q^i} \\ \Leftrightarrow (\alpha - \alpha^{q^k})^{q^i} &= 0 \\ \Leftrightarrow \alpha &= \alpha^{q^k}. \end{aligned}$$

We also know that f divides $x^{q^k} - x$ by the minimality of f. By proposition 8.0.2 we have that $d|k$. By assumption we have that $0 \leq k < d$, so we must have $k = 0$ as was to be shown.

b) It follows from a) that $a_1 = Tr_{\mathbb{E}/\mathbb{F}}(\alpha)$ and $a_d = N_{\mathbb{E}/\mathbb{F}}(\alpha)$. Since by construction $\alpha \in \mathbb{E}$, we have $Tr_{\mathbb{K}/\mathbb{E}}(\alpha) = [\mathbb{K} : \mathbb{E}]\alpha = \frac{n}{d}\alpha$ and $N_{\mathbb{K}/\mathbb{E}}(\alpha) = \alpha^{\frac{n}{d}}$. By proposition 8.0.4, we have

$$Tr_{\mathbb{K}/\mathbb{F}}(\alpha) = Tr_{\mathbb{E}/\mathbb{F}}(Tr_{\mathbb{K}/\mathbb{E}}(\alpha)) = \frac{n}{d}Tr_{\mathbb{E}/\mathbb{F}}(\alpha) = Tr_{\mathbb{E}/\mathbb{F}}\left(\frac{n}{d}\alpha\right) = \frac{n}{d}a_1$$

as the trace function is additive.

c) Analogously:

$$N_{\mathbb{K}/\mathbb{F}}(\alpha) = N_{\mathbb{E}/\mathbb{F}}(N_{\mathbb{K}/\mathbb{E}}(\alpha)) = N_{\mathbb{E}/\mathbb{F}}(\alpha)^{\frac{n}{d}} = N_{\mathbb{E}/\mathbb{F}}(\alpha^{\frac{n}{d}}) = a_d^{\frac{n}{d}}$$

as the norm function is multiplicative. This completes the proof. □

From these basic algebraic results, we are ready to introduce some lemmas. First, let us state the important Hasse-Davenport relation, which we wish to prove:

Theorem 8.0.6. *The Hasse-Davenport relation:*
Let $\mathbb{F}$ be the field with q elements and let $\mathbb{E}$ be an extension of $\mathbb{F}$ of degree s. For g a Gauss sum, χ a character on $\mathbb{F}$ and χ' a character on $\mathbb{E}$ as in definition 8.0.1, it holds that

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

We will give a proof of this at the end of the chapter, but this proof requires several lemmas which we will introduce first. Initially when we introduced Gauss sums, we did so on the form

$$g_a(\chi) = \sum_{t \in \mathbb{F}_p} \chi(t) e^{at\frac{2i\pi}{p}} = \sum_{t \in \mathbb{F}_p} \chi(t)\zeta^{at}$$

where we denoted g_1 simply as g. Let $\mathbb{E}, \mathbb{F}$ and $\mathbb{F}_p$ be finite fields such that $\mathbb{F}_p \subset \mathbb{F} \subset \mathbb{E}$. Let $\mathbb{F}_p, \mathbb{F}$ and $\mathbb{E}$ have respectively p, q and q^s elements. In the following, we consider $\xi(t) = \zeta_p^{Tr(t)}$, where the trace $Tr(t)$ is given as the function $Tr_{\mathbb{F}/\mathbb{F}_p}(t)$ as in definition 8.0.3. Then we have that

$$g(\chi') = \sum_{t \in \mathbb{E}} \chi'(t)\xi'(t)$$

for $\xi' = \zeta^{Tr_{\mathbb{E}/\mathbb{F}}(t)}$. By proposition 8.0.4,

$$Tr_{\mathbb{E}/\mathbb{F}_p}(t) = Tr_{\mathbb{F}/\mathbb{F}_p}(Tr_{\mathbb{E}/\mathbb{F}}(t))$$

and so $\xi' = \xi \circ Tr_{\mathbb{E}/\mathbb{F}}$.

Let $f(x) \in \mathbb{F}[x]$ be a monic polynomial, and write $f(x) = x^n - a_1x^{n-1} + ... + (-1)^n a_n$. We now define $\lambda : \mathbb{F}[x] \to \mathbb{C}$ by $\lambda(f) = \xi(a_1)\chi(a_n)$. This λ-function will become useful in proving the Hasse-Davenport relation, so now we will go over some lemmas concerning the properties of λ:

Lemma 8.0.7. *For monic polynomials f and g in $\mathbb{F}[x]$, λ as given above is a multiplicative function, i.e.*

$$\lambda(fg) = \lambda(f)\lambda(g).$$

Proof. Let

$$\begin{aligned} f(x) &= x^n - a_1x^{n-1} + ... + (-1)^n a_n \\ g(x) &= x^m - b_1x^{m-1} + ... + (-1)^m b_m. \end{aligned}$$

Then their product is given by

$$f(x)g(x) = x^{m+n} - (a_1 + b_1)x^{m+n-1} + ... + (-1)^{n+m} a_n b_m.$$

By applying λ and noting that by definition $\xi(a + b) = \xi(a)\xi(b)$, we see that

$$\lambda(fg) = \xi(a_1 + b_1)\chi(a_n b_m) = \xi(b_1)\xi(a_1)\chi(b_m)\chi(a_n) = \lambda(f)\lambda(g)$$

as wanted. □

Lemma 8.0.8. *Let α be an element of the finite field $\mathbb{E}$, and let f be the minimal polynomial for α over $\mathbb{F}$. Let $d = \deg(f)$ and let $\mathbb{E}$ be an extension of degree s over $\mathbb{F}$. Then we have that*

$$\lambda(f)^{\frac{s}{d}} = \chi'(\alpha)\xi'(\alpha).$$

Proof. We can apply proposition 8.0.5 for $f(x) = x^d - a_1x^{d-1} + ... + (-1)^d a_d$, so we have that

$$\begin{aligned} Tr_{\mathbb{E}/\mathbb{F}}(\alpha) &= \frac{s}{d} a_1 \\ N_{\mathbb{E}/\mathbb{F}}(\alpha) &= a_d^{\frac{s}{d}}. \end{aligned}$$

By definition, $\lambda(f) = \xi(a_1)\chi(a_d)$, so by raising both sides to the power $\frac{s}{d}$, we get

$$\begin{aligned} \lambda(f)^{\frac{s}{d}} &= \xi(a_1)^{\frac{s}{d}}\chi(a_d)^{\frac{s}{d}} \\ &= \xi\left(\frac{s}{d}a_1\right)\chi\left(a_d^{\frac{s}{d}}\right) \\ &= \xi(Tr_{\mathbb{E}/\mathbb{F}}(\alpha))\chi(N_{\mathbb{E}/\mathbb{F}}(\alpha)) \\ &= \xi'(\alpha)\chi'(\alpha). \end{aligned}$$

□

We now prove one final lemma involving the λ function defined above before moving onto the proof of Hasse-Davenport.

Lemma 8.0.9. *Let $\mathbb{F}$ be the field with q elements and let $\mathbb{E}$ be a field extension of $\mathbb{F}$ of degree s. Let g be the Gauss sum over χ'. Then*

$$g(\chi') = \sum_f \deg(f)\lambda(f)^{\frac{s}{\deg(f)}}$$

where the sum is over all monic irreducible polynomials in $\mathbb{F}[x]$ of degree dividing s.

Proof. If we take $\mathbb{F}$ as our base field in proposition 8.0.2, then we know $x^{q^s} - x$ can be written as a product of all the monic irreducible polynomials in $\mathbb{F}[x]$ with order dividing s. Each of these monic irreducible polynomials will have all its roots in $\mathbb{E}$, and similarly every $\alpha \in \mathbb{E}$ will be a root of such a monic irreducible polynomial.
Now let $f(x) \in \mathbb{F}[x]$ be monic and irreducible, with $\deg(f) = d$ and $d|s$. Denote the roots of f by $\alpha_1, ..., \alpha_d$, all of which lie in $\mathbb{E}$. Lemma 8.0.8 gives that

$$d\lambda(f)^{\frac{s}{d}} = \sum_{i=1}^{d} \chi'(\alpha_i)\xi'(\alpha_i).$$

If we sum over all monic irreducible polynomials of order dividing s, we precisely get that $g(\chi') = \sum\limits_{t\in\mathbb{E}} \chi'(t)\xi'(t) = \sum\limits_f \deg(f)\lambda(f)^{\frac{s}{\deg(f)}}$ as wanted. □

We are now ready for the main result of the chapter:

Proof. (Of Hasse-Davenport)
We start by looking at the sum $\sum_f \lambda(f)t^{\deg(f)}$. We wish to show that

$$\sum_f \lambda(f)t^{\deg(f)} = \frac{1}{\prod_f (1 - \lambda(f)t^{\deg(f)})}$$

where the sum is over all monic polynomials and the product is over all monic irreducible polynomials in $\mathbb{F}[x]$, where $\mathbb{F}$ is the finite field with q elements. This follows by calculation:

$$\begin{aligned}
& \prod_{monic\ irreducible\ f} \frac{1}{1-\lambda(f)t^{\deg(f)}} \\
= \; & \frac{1}{1-\lambda(f_1)t^{\deg(f_1)}} \cdot \frac{1}{1-\lambda(f_2)t^{\deg(f_2)}} \cdot ... \\
= \; & \sum_{k=0}^{\infty} \left(\lambda(f_1)t^{\deg(f_1)}\right)^k \cdot \sum_{k=0}^{\infty} \left(\lambda(f_2)t^{\deg(f_2)}\right)^k \cdot ... \\
= \; & (\lambda(f_1)t^{\deg(f_1)} + \lambda^2(f_1)t^{2\deg(f_1)} + ...) \cdot (\lambda(f_2)t^{\deg(f_2)} + \lambda^2(f_2)t^{2\deg(f_2)} + ...) \cdot ... \\
= \; & \sum_{monic\ f} \lambda(f)t^{\deg(f)}
\end{aligned}$$

using the fact that any monic polynomial can be written uniquely as the product of monic irreducible polynomials. This is also equivalent to:

$$\sum_f \lambda(f)t^{\deg(f)} = \sum_{s\in\mathbb{N}_0} \left(\sum_{deg(f)=s} \lambda(f) \right) t^s$$

where we define $\lambda(1) = 1$. We see that the term corresponding to $s = 0$ is equal to 1. Next, we consider the cases $s = 1$ and $s > 1$ separately. For $s = 1$, we have that:

$$\begin{aligned}
\sum_{\deg(f)=1} \lambda(f) &= \sum_{a\in\mathbb{F}} \lambda(x-a) \\
&= \sum_{a\in\mathbb{F}} \chi(a)\xi(a) \\
&= g(\chi)
\end{aligned}$$

by definition of λ. For $s > 1$, we get that:

$$\begin{aligned}
\sum_{\deg(f)=s,\ s>1} \lambda(f) &= \sum_{a_i\in\mathbb{F}} \lambda(x^s - a_1x^{s-1} + ... + (-1)^s a_s) \\
&= q^{s-2} \sum_{a_1,a_s\in\mathbb{F}} \chi(a_s)\xi(a_1) \\
&= q^{s-2} \left(\sum_{a_s\in\mathbb{F}} \chi(a_s) \right) \left(\sum_{a_1\in\mathbb{F}} \xi(a_1) \right) \\
&= 0
\end{aligned}$$

by proposition 2.1.3. We then have that

$$\sum_f \lambda(f)t^{\deg(f)} = 1 \cdot t^0 + g(\chi)t + 0 = 1 + g(\chi)t.$$

We now apply logarithmic differentiation:

$$\frac{d}{dt} \log \left(\sum_f \lambda(f)t^{\deg(f)} \right) = \frac{d}{dt} \log \left(\frac{1}{\prod_f (1-\lambda(f)t^{\deg(f)})} \right)$$

which gives

$$\frac{g(\chi)}{1+g(\chi)t} = \frac{\lambda(f)\deg(f)t^{\deg(f)-1}}{1-\lambda(f)t^{\deg(f)}}$$

which is equivalent to

$$\frac{g(\chi)t}{1+g(\chi)t} = \frac{\lambda(f)\deg(f)t^{\deg(f)}}{1-\lambda(f)t^{\deg(f)}}$$

by multiplication with t. We expand the denominators into geometric series:

$$\begin{aligned}\frac{1}{1+g(\chi)} &= \sum_{s=0}^{\infty}(-g(\chi)t)^s \\ &= \sum_{s=0}^{\infty}(-1)^s g(\chi)^s t^s,\end{aligned}$$

so that

$$\begin{aligned}\frac{g(\chi)t}{1+g(\chi)} &= \sum_{s=0}^{\infty}(-1)^s g(\chi)^{s+1} t^{s+1} \\ &= \sum_{s=1}^{\infty}(-1)^{s-1} g(\chi)^s t^s.\end{aligned}$$

Similarly,

$$\frac{1}{1-\lambda(f)t^{\deg(f)}} = \sum_{r=0}^{\infty}\lambda(f)^r t^{r\deg(f)},$$

so that

$$\frac{\lambda(f)\deg(f)t^{\deg(f)}}{1-\lambda(f)t^{\deg(f)}} = \sum_{r=0}^{\infty}\deg(f)\lambda(f)^{r+1}t^{(r+1)\deg(f)}$$

which gives the expression

$$\sum_f \frac{\lambda(f)\deg(f)t^{\deg(f)}}{1-\lambda(f)t^{\deg(f)}} = \sum_f \sum_{r=1}^{\infty}\deg(f)\lambda(f)^r t^{r\deg(f)}.$$

To finish the proof, we can now equate the coefficients of t^s and get

$$(-1)^{s-1}g(\chi)^s = \sum_{\deg(f)|s}\deg(f)\lambda(f)^{\frac{s}{\deg(f)}}.$$

By lemma 8.0.9, we have that $g(\chi') = \sum_{\deg(f)|s}\deg(f)\lambda(f)^{\frac{s}{\deg(f)}}$. Thus $(-1)^s g(\chi)^s = (-g(\chi))^s = -g(\chi')$, which gives the Hasse-Davenport identity. □

The general case: $a_0x_0^{n_0} + ... + a_rx_r^{n_r} = b$

In this chapter we will study the most general type of equation over a finite field $\mathbb{F}$ with p elements, namely the one given by

$$a_0x_0^{n_0} + ... + a_rx_r^{n_r} = b.$$

Theorem 9.0.1. *Let $a_0, ..., a_r \in \mathbb{F}_p^*$, $n_0, ..., n_r \in \mathbb{N}$ and $b \in \mathbb{F}_p$. Let $n_i|(p-1)$ for $i = 0, ..., r$. Over $\mathbb{F}_p$ we have the following identities for the number of solutions to $a_0x_0^{n_0} + ... + a_rx_r^{n_r} = b$ for respectively $b = 0$ and $b \neq 0$:*

a) $N(a_0x_0^{n_0} + ... + a_rx_r^{n_r} = 0) = p^r + \sum \chi_0(a_0^{-1}) \cdot ... \cdot \chi_r(a_r^{-1})J_0(\chi_0, ..., \chi_r)$

where the sum is taken over tuples $(\chi_0, ..., \chi_r)$ of characters on $\mathbb{F}_p$ such that $\chi_i^{n_i} = \varepsilon$, $\chi_i \neq \varepsilon$ for $i = 0, .., r$ and $\chi_0 \cdot ... \cdot \chi_r = \varepsilon$.

b) $N(a_0x_0^{n_0} + ... + a_rx_r^{n_r} = b) = p^r + \sum \chi_0 \cdot ... \cdot \chi_r(b)\chi_0(a_0^{-1}) \cdot ... \cdot \chi_r(a_r^{-1})J(\chi_0, ..., \chi_r)$

where the sum is taken over tuples $(\chi_0, ..., \chi_r)$ of characters on $\mathbb{F}_p$ such that $\chi_i^{n_i} = \varepsilon$, $\chi_i \neq \varepsilon$ for $i = 0, .., r$.

Proof. a) We first use the decomposition

$$N(a_0x_0^{n_0} + ... + a_rx_r^{n_r} = 0) = \sum_{a_0u_0+...+a_ru_r=0} N(x_0^{n_0} = u_0) \cdot ... \cdot N(x_r^{n_r} = u_r).$$

We can rewrite each factor as $N(x_i^{n_i} = u_i) = \sum\limits_{\chi_i} \chi_i(u_i)$ by letting χ_i run over all characters of order dividing n_i. We then apply the substitution $t_i = a_iu_i$, so we get

$$\begin{aligned}
&\sum_{a_0u_0+...+a_ru_r=0} N(x_0^{n_0} = u_0) \cdot ... \cdot N(x_r^{n_r} = u_r) \\
= &\sum_{\chi_0,...,\chi_r} \sum_{a_0u_0+...+a_ru_r=0} \chi_0(u_0) \cdot ... \cdot \chi_r(u_r) \\
= &\sum_{\chi_0,...,\chi_r} \sum_{t_0+...+t_r=0} \chi_0(t_0) \cdot ... \cdot \chi_r(t_r)\chi_0(a_0^{-1}) \cdot ... \cdot \chi_r(a_r^{-1}) \\
= &\sum_{\chi_0,...,\chi_r} \chi_0(a_0^{-1}) \cdot ... \cdot \chi_r(a_r^{-1})J_0(\chi_0, ..., \chi_r)
\end{aligned}$$

by the previous definition of J_0. If $\chi_i = \varepsilon$ for all i, $\chi_0(a_0^{-1}) \cdot ... \cdot \chi_r(a_r^{-1})J_0(\chi_0, ..., \chi_r)$ is equal to p^r by theorem 4.0.2. If for some, but not all i, $\chi_i = \varepsilon$, the term is equal to zero.

Hence the only other non-zero contribution is for $\chi_0 \cdot ... \cdot \chi_r = \varepsilon$. This proves identity a).
b) again we decompose into

$$N(a_0 x_0^{n_0} + ... + a_r x_r^{n_r} = b) = \sum_{a_0 u_0 + ... + a_r u_r = b} N(x_0^{n_0} = u_0) \cdot ... \cdot N(x_r^{n_r} = u_r).$$

As in case a), we rewrite each factor as $N(x_i^{n_i} = u_i) = \sum_{\chi_i} \chi_i(u_i)$. We then apply the substitution $t_i = b^{-1} a_i u_i$ and get

$$\begin{aligned}
&\sum_{a_0 u_0 + ... + a_r u_r = b} N(x_0^{n_0} = u_0) \cdot ... \cdot N(x_r^{n_r} = u_r) \\
&= \sum_{\chi_0, ..., \chi_r} \sum_{a_0 u_0 + ... + a_r u_r = b} \chi_0(u_0) \cdot ... \cdot \chi_r(u_r) \\
&= \sum_{\chi_0, ..., \chi_r} \sum_{a_0 b t_0 a_0^{-1} + ... + a_r b t_r a_r^{-1} = b} \chi_0 \cdot ... \cdot \chi_r(b) \chi_0(a_0^{-1}) \cdot ... \cdot \chi_r(a_r^{-1}) \chi_0(t_0) \cdot ... \cdot \chi_r(t_r) \\
&= \sum_{\chi_0, ..., \chi_r} \sum_{t_0 + ... + t_r = 1} \chi_0 \cdot ... \cdot \chi_r(b) \chi_0(a_0^{-1}) \cdot ... \cdot \chi_r(a_r^{-1}) \chi_0(t_0) \cdot ... \cdot \chi_r(t_r) \\
&= \sum_{\chi_0, ..., \chi_r} \chi_0 \cdot ... \cdot \chi_r(b) \chi_0(a_0^{-1}) \cdot ... \cdot \chi_r(a_r^{-1}) J(\chi_0, ..., \chi_r).
\end{aligned}$$

For $\chi_i = \varepsilon$ for all i, the term $\chi_0 \cdot ... \cdot \chi_r(b) \chi_0(a_0^{-1}) \cdot ... \cdot \chi_r(a_r^{-1}) J(\chi_0, ..., \chi_r)$ is equal to p^r, again by theorem 4.0.2. If some, but not all, $\chi_i = \varepsilon$, the term is equal to zero. This proves b). □

We will now look at case a) over projective space, for $n_0 = ... = n_r = n$ where $n|(p-1)$. For simplicity, let $N = N(a_0 x_0^n + ... + a_r x_r^n = 0)$. Let $\overline{N}$ denote the number of solutions over projective space. Then we know $N = \overline{N}(p-1) + 1$, i.e. $\overline{N} = \frac{N-1}{p-1}$. As we have shown

$$N = p^n + \sum_{\chi_0, ..., \chi_r} \overline{\chi_0}(a_0) \cdot ... \cdot \overline{\chi_r}(a_r) J_0(\chi_0, ..., \chi_r)$$

we then get, by definition of $\overline{N}$:

$$\overline{N} = p^{r-1} + ... + p + 1 + \frac{1}{p-1} \sum_{\chi_0, ..., \chi_r} \overline{\chi_0}(a_0) \cdot ... \cdot \overline{\chi_r}(a_r) J_0(\chi_0, ..., \chi_r).$$

Before we proceed, it is useful to show the following lemma:

Lemma 9.0.2. *We have the following relation between Gauss sums and J_0:*

$$\frac{1}{p-1} J_0(\chi_0, ..., \chi_r) = \frac{1}{p} g(\chi_0) \cdot ... \cdot g(\chi_r).$$

Proof. By theorem 4.0.2, we have that

$$\begin{aligned}
\frac{1}{p-1} J_0(\chi_0, ..., \chi_r) &= \frac{1}{p-1} \chi_r(-1)(p-1) J(\chi_0, ..., \chi_{r-1}) \\
&= \frac{1}{p-1} \chi_r(-1)(p-1) J(\chi_0, ..., \chi_{r-1}) \frac{g(\chi_r)}{g(\chi_r)} \\
&= \chi_r(-1) \frac{g(\chi_0) \cdot ... \cdot g(\chi_r)}{g(\chi_0 \cdot ... \cdot \chi_{r-1}) g(\chi_r)}.
\end{aligned}$$

By corollary 4.0.3.1, $g(\chi_0, ..., \chi_{r-1})g(\chi_r) = \chi_r(-1)p$, hence

$$\begin{aligned}\frac{1}{p-1}J_0(\chi_0 ... \chi_r) &= \frac{\chi_r(-1)g(\chi_0)\cdot ... \cdot g(\chi_r)}{\chi_r(-1)p} \\ &= \frac{1}{p}g(\chi_0)\cdot ... \cdot g(\chi_r).\end{aligned}$$

□

9.1 The rationality of the generating function for N

Let $\mathbb{F}$ be the field with p elements and let $\mathbb{K}$ be an extension of $\mathbb{F}$ of degree k. Again we consider the equation

$$a_0x_0^n + ... + a_rx_r^n = 0, \ n|(p-1).$$

Let $\overline{N}_k$ denote the number of projective solutions over $\mathbb{K}$. Then we have that

$$\begin{aligned}\overline{N}_k &= 1 + p^k + ... + p^{k(r-1)} + \sum_{\chi_0', ..., \chi_r'} \overline{\chi_0'}(a_0)\cdot ... \cdot \overline{\chi_r}(a_r)\frac{1}{p^k}g(\chi_0')\cdot ... \cdot g(\chi_r') \\ &= 1 + p^k + ... + p^{k(r-1)} + (-1)^{r+1}\sum_{\chi_0, ..., \chi_r} \overline{\chi_0}^k(a_0)\cdot ... \cdot \overline{\chi_r}^k(a_r)\frac{1}{p^k}(-1)^{k(r+1)}g^k(\chi_0)\cdot ... \cdot g^k(\chi_r)\end{aligned}$$

by definition of the extended characters χ_i' and use of Hasse-Davenport. We wish to show the following theorem:

Theorem 9.1.1. *Let u be our variable, and let $\sum_{k=1}^{\infty} N_ku^k$ be the generating function for the number of solutions to the equation $a_0x_0^n + ... + a_rx_r^n = 0$ over the finite field $\mathbb{K}$. Then this generating series is a rational function of u.*

Proof. First we note that it is enough to consider the generating function for $\overline{N}_k$, by the linear relation $N = \overline{N}(p-1) + 1$. We will proceed by showing that the generating function $\sum_{k=1}^{\infty} \overline{N}_ku^{k-1}$ gives a rational function of u. We calculate the value of $\sum_{k=1}^{\infty} \overline{N}_ku^{k-1}$:

$$\begin{aligned}&\sum_{k=1}^{\infty} \overline{N}_ku^{k-1} \\ = &\sum_{k=1}^{\infty}\sum_{j=0}^{r-1} p^{jk}u^{k-1} + (-1)^{r+1}\sum_{k=1}^{\infty}\sum_{\chi_0, ..., \chi_r} \overline{\chi_0}^k(a_0)\cdot ... \cdot \overline{\chi_r}^k(a_r)\frac{1}{p^k}(-1)^{k(r+1)}g^k(\chi_0)\cdot ... \cdot g^k(\chi_r)u^{k-1}.\end{aligned}$$

To simplify this, we look at $\overline{\chi_0}^k(a_0)\cdot ... \cdot \overline{\chi_r}^k(a_r)\frac{1}{p^k}(-1)^{k(r+1)}g^k(\chi_0)\cdot ... \cdot g^k(\chi_r)$. We have that

$$\begin{aligned} & \overline{\chi_0}^k(a_0)\cdot \ldots \cdot \overline{\chi_r}^k(a_r)\frac{1}{p^k}(-1)^{k(r+1)}g^k(\chi_0)\cdot \ldots \cdot g^k(\chi_r) \\ = & \left(\overline{\chi_0}(a_0)\cdot \ldots \cdot \overline{\chi_r}(a_r)\frac{1}{p}(-1)^{r+1}g(\chi_0)\cdot \ldots \cdot g(\chi_r)\right)^k \\ = & \left((-1)^{r+1}\overline{\chi_0}(a_0)\cdot \ldots \cdot \overline{\chi_r}(a_r)\frac{1}{p-1}J_0(\chi_0, \ldots, \chi_r)\right)^k \\ = & (C(-1)^{-2})^k \\ = & C^k \end{aligned}$$

where we put

$$C = (-1)^{r-1}\overline{\chi_0}(a_0)\cdot \ldots \cdot \overline{\chi_r}(a_r)\frac{1}{p-1}J_0(\chi_0, \ldots, \chi_r).$$

Then

$$\begin{aligned} \sum_{k=1}^{\infty}\overline{N}_k u^{k-1} &= \sum_{k=1}^{\infty}\sum_{j=0}^{r-1}p^{jk}u^{k-1} + (-1)^{r+1}\sum_{k=1}^{\infty}\sum_{\chi_0,\ldots,\chi_r}C^k u^{k-1} \\ &= -\sum_{j=0}^{r-1}\frac{d}{du}\log(1-p^j u) + (-1)^r\sum_{\chi_0,\ldots,\chi_r}\frac{d}{du}\log(1-Cu) \end{aligned}$$

since we have

$$\begin{aligned} -\sum_{j=0}^{r-1}\frac{d}{du}\log(1-p^j u) &= (-1)^2\sum_{j=0}^{r-1}\sum_{m=1}^{\infty}\frac{d}{du}(-1)^m\frac{(-p^j u)^m}{m} \\ &= \sum_{j=0}^{r-1}\sum_{m=1}^{\infty}\frac{d}{du}(-1)^{2m}\frac{p^{jm}u^m}{m} \\ &= \sum_{j=0}^{r-1}\sum_{m=1}^{\infty}p^{jm}u^{m-1} \end{aligned}$$

and

$$\begin{aligned} (-1)^r\sum_{\chi_0,\ldots,\chi_r}\frac{d}{du}\log(1-Cu) &= (-1)^{r+1}\sum_{\chi_0,\ldots,\chi_r}\sum_{m=1}^{\infty}\frac{d}{du}(-1)^m\frac{(-Cu)^m}{m} \\ &= (-1)^{r+1}\sum_{\chi_0,\ldots,\chi_r}\sum_{m=1}^{\infty}\frac{d}{du}(-1)^{2m}\frac{C^m u^m}{m} \\ &= (-1)^{r+1}\sum_{\chi_0,\ldots,\chi_r}\sum_{m=1}^{\infty}C^m u^{m-1}. \end{aligned}$$

What remains is to show the rationality in u:

$$\begin{aligned}
\sum_{k=1}^{\infty} \overline{N}_k u^{k-1} &= -\sum_{j=0}^{r-1} \frac{d}{du} \log(1-p^j u) + (-1)^r \sum_{\chi_0,\ldots,\chi_r} \frac{d}{du} \log(1-Cu) \\
&= -\frac{d}{du} \log \left(\prod_{j=0}^{r-1} (1-p^j u) \right) + (-1)^r \frac{d}{du} \log \left(\prod_{\chi_0,\ldots,\chi_r} (1-Cu) \right) \\
&= \frac{d}{du} \log \left(\frac{1}{\prod\limits_{j=0}^{r-1} (1-p^j u)} \right) + \frac{d}{du} \log \left(\left(\prod_{\chi_0,\ldots,\chi_r} (1-Cu) \right)^{(-1)^r} \right) \\
&= \frac{d}{du} \log \left(\frac{\left(\prod\limits_{\chi_0,\ldots,\chi_r} (1-Cu) \right)^{(-1)^r}}{\prod\limits_{j=0}^{r-1} (1-p^j u)} \right).
\end{aligned}$$

This gives a rational function, since the derivative $\frac{d}{dx} \log(x) = \frac{1}{x}$ is rational, and we only work with finite products in the above. □

Conclusion

Throughout this thesis we have treated different types of equations over finite fields, and as we have seen, they can be analyzed using several different methods. Some of these methods have the benefit of simplicity, others that they lead to additional theorems and results in the process.
The final result of weil's is quite noteworthy; when we look at the number of solutions to a general Fermat hypersurface, we can associate this to a finite and rational function regardless of the degree of the field extension we work with. One of the further results one can show is that the results in chapter 8 also hold without the assumption $n|(p-1)$. No doubt it is possible to generalize this theory even further, or consider other interesting special cases, though even within the limitations we have worked with here, we have found many broad and useful results.

Bibliography

[1] Dummit, David S. and Foote, Richard M.: *Abstract Algebra.* 3. ed. Wiley, 2004.

[2] Milne, J.S.: *Algebraic Number Theory.* 3. ed. Springer, 1995.

[3] Rosen, Michael and Ireland, Kenneth: *A Classical Introduction to Modern Number Theory.* 2. ed. Springer, 1990.

[4] Silverman, Joseph H. and Tate, John. T.: *Rational Points on Elliptic Curves.* 2. ed. Springer, 2015.

[5] Weil, André: *Numbers of Solutions of Equations in Finite Fields.* Journal: Bull. Amer. Math. Soc. 55 (1949), p.497-508.