Introduction

Denote by \( q \) an odd prime power, and let \( X(\mathbb{F}_q^*) := \text{Hom}(\mathbb{F}_q^*, \mathbb{C}^*) \) be the group of multiplicative characters on the finite field \( \mathbb{F}_q \) with \( q \) elements. We denote by \( \mu_q \in X(\mathbb{F}_q^*) \) the quadratic character on \( \mathbb{F}_q \), i.e. the unique character of order 2, and we denote by \( \epsilon \in X(\mathbb{F}_q^*) \) the trivial character. We extend the domain of a multiplicative character from \( \mathbb{F}_q^* \) to \( \mathbb{F}_q \) by setting \( \chi(0) = 0 \) if \( \chi \in X(\mathbb{F}_q^*) \) is nontrivial and \( \epsilon(0) = 1 \).

In this paper we consider Legendre sums, which are character sums of the form

\[
S_q(\chi; b) := \sum_{x \in \mathbb{F}_q} \chi(x) \mu_q(Q_b(x)),
\]

where \( b \in \mathbb{F}_q, \chi \in X(\mathbb{F}_q^*) \), and \( Q_b = T^2 + 2bT + 1 \in \mathbb{F}_q[T] \). In Proposition 1.2.2, we show that \( S_q(\chi; b) \) is real.

In Theorem 2.0.1 we prove a “Hasse-Davenport” relation for Legendre sums, and as a corollary we obtain the bound \( |S_q(\chi; b)| \leq 2\sqrt{q} \) for \( b \in \mathbb{F}_q^* \setminus \{\pm 1\} \) and nontrivial \( \chi \in X(\mathbb{F}_q^*) \). This allows us to define a unique angle \( \theta \in [0, \pi] \) associated to the pair \( (\chi, b) \) by the equation

\[
S_q(\chi; b) = 2\sqrt{q} \cos(\theta).
\]

We attempt to study the distribution of these angles as \( q \to \infty \) for fixed \( b \) and varying \( \chi \). In particular, we prove the following result.

**Theorem 0.0.1.** Let \( \{q_m\}_{m \geq 1} \) be a sequence of odd prime powers which tends to infinity. For a given \( m \) and all \( \chi \in X(\mathbb{F}_{q_m}^*) \) let \( \theta_{\chi} \) be the angle associated to the Legendre sum \( S_{q_m}(\chi; 0) \). Then the numbers \( \{\theta_{\chi}\}_{\chi \in X(\mathbb{F}_{q_m}^*)} \) become equidistributed with respect to
the measure which is the average of the Haar measure on 
\([0, \pi]\) and the Dirac delta measure at \(\pi/2\) as \(m \to \infty\), i.e. for all continuous maps \(f : [0, \pi] \to \mathbb{R}\),

\[
\lim_{m \to \infty} \frac{1}{q_m - 1} \sum_{\chi \in X(F_{q_m}^*)} f(\theta_\chi) = \frac{1}{2\pi} \int_0^\pi f(\theta) \, d\theta + \frac{1}{2} f\left(\frac{\pi}{2}\right).
\]

We motivate this theorem with the following graph. The angles corresponding to the Legendre sums \(S_{114}(\chi; 0)\) for \(\chi\) varying over all \(\chi \in X(F_{114}^*)\) were computed, and a histogram of them was plotted. Furthermore, overlaid on the graph is the constant line \(\theta \mapsto \frac{1}{2\pi}\).

Furthermore, we reduce the following conjecture to the problem of proving that a particular infinite product converges to a polynomial.

**Conjecture 0.0.2.** Let \(\{q_m\}_{m \geq 1}\) be a sequence of odd prime powers which tends to infinity. For all \(m \geq 1\) take \(b \in \mathbb{F}_{q_m} \setminus \{0, 1, -1\}\), and for all \(\chi \in X(F_{q_m}^*)\), let \(\theta_\chi\) be the angle associated to the Legendre sum \(S_{q_m}(\chi; b_m)\). Then the numbers \(\{\theta_\chi\}_{\chi \in X(F_{q_m}^*)}\) become equidistributed with respect to the Sato-Tate measure on \([0, \pi]\) as \(m \to \infty\), i.e.

for all continuous maps \(f : [0, \pi] \to \mathbb{R}\),

\[
\lim_{m \to \infty} \frac{1}{q_m - 1} \sum_{\chi \in X(F_{q_m}^*)} f(\theta_\chi) = \frac{2}{\pi} \int_0^\pi f(\theta) \sin^2(\theta) \, d\theta.
\]

We motivate this conjecture with the following set of graphs. The angles corresponding to the Legendre sums \(S_q(\chi; b)\) for \(q = 11^3, 11^4, 11^5\), fixing \(b = 2\) and varying \(\chi\) over all \(\chi \in X(F_q^*)\), were computed, and histograms of them were plotted. Furthermore, overlaid on each graph is the curve of the function \(\theta \mapsto \frac{2}{\pi}\sin^2(\theta)\).
Histogram of angles for $q = 11^3$

Histogram of angles for $q = 11^4$
1 Legendre Character Sums

In this section we discuss some properties of multiplicative characters and derive some elementary properties of Legendre sums.

1.1 Characters and Character Lifting

The group $X(\mathbb{F}_q^*)$ of multiplicative characters on $\mathbb{F}_q$ is a cyclic group of order $q - 1$ and is hence isomorphic to $\mathbb{F}_q^*$. Recall the following orthogonality relations. For $a \in \mathbb{F}_q^*$, we have the identity

$$\sum_{\chi \in X(\mathbb{F}_q^*)} \chi(a) = \begin{cases} q - 1, & a = 1, \\ 0, & a \neq 1 \end{cases}. \quad (1.1.1)$$

and for $\chi \in X(\mathbb{F}_q^*)$, we have the identity

$$\sum_{a \in \mathbb{F}_q} \chi(a) = \begin{cases} q, & \chi = \epsilon, \\ 0, & \chi \neq \epsilon \end{cases}. \quad (1.1.2)$$

Also recall that for $a \in \mathbb{F}_q$, if $d \mid q - 1$, then

$$\# \{ x \in \mathbb{F}_q : x^d = a \} = \sum_{\chi \in X(\mathbb{F}_q^*)} \chi(a), \quad (1.1.3)$$
Proposition 1.1.5. Consider $\chi \in X(F_q^*)$. If $\chi$ is square, then $\chi(-1) = 1$, and if $\chi$ is non-square, then $\chi(-1) = -1$.

Proof. Let $g$ be the generator of $F_q^*$. We note that the character $\chi_0 \in X(F_q^*)$ determined by $\chi_0(g) = e^{2\pi i/(q-1)}$ has order $q-1$ and hence generates $X(F_q^*)$. Furthermore, $\chi_0(-1) = \chi_0(g^{(q-1)/2}) = \chi_0(g)^{(q-1)/2} = e^{\pi i} = -1$.

If $\chi$ is square, then $\chi = \chi_0^k$ for some even integer $k$. Then $\chi(-1) = \chi_0(-1)^k = (-1)^k = 1$. If $\chi$ is non-square, then $\chi = \chi_0^l$ for some odd integer $l$. Then $\chi(-1) = \chi_0(-1)^l = (-1)^l = -1$. ☐

Let $n$ be a positive integer. Let $N_{F_q^n/F_q}$ be the norm of the field extension $F_q^n/F_q$, given by

$$N_{F_q^n/F_q}(\alpha) = \prod_{k=0}^{n-1} \alpha^k.$$

for $\alpha \in F_q^n$. We recall the following properties of the norm.

Proposition 1.1.6. The norm $N_{F_q^n/F_q}$ maps $F_q^*$ onto $F_q^*$. Furthermore, if we take $\alpha, \beta \in F_q^n$ and $x \in F_q$, then

$$N_{F_q^n/F_q}(\alpha) \in F_q,$$

$$N_{F_q^n/F_q}(\alpha \beta) = N_{F_q^n/F_q}(\alpha) N_{F_q^n/F_q}(\beta),$$

$$N_{F_q^n/F_q}(\alpha x) = x^n N_{F_q^n/F_q}(\alpha).$$

Similarly, let $Tr_{F_q^n/F_q}$ be the trace of the field extension $F_q^n/F_q$, given by

$$Tr_{F_q^n/F_q}(\alpha) = \sum_{k=0}^{n-1} \alpha^k.$$

We recall the following properties of the trace.

Proposition 1.1.7. The trace $Tr_{F_q^n/F_q}$ maps $F_q^n$ onto $F_q$. Furthermore, if we take $\alpha, \beta \in F_q^n$ and $x \in F_q$, then

$$Tr_{F_q^n/F_q}(\alpha) \in F_q,$$

$$Tr_{F_q^n/F_q}(\alpha + \beta) = Tr_{F_q^n/F_q}(\alpha) + Tr_{F_q^n/F_q}(\beta),$$

$$Tr_{F_q^n/F_q}(\alpha x) = x Tr_{F_q^n/F_q}(\alpha).$$

For proofs of the properties of the norm and trace see Chapter 11.2 of [1].

Let $\chi$ be a multiplicative character on $F_q$. Proposition 1.1.6 allows us to lift $\chi$ to a character on $F_q^n$ by composing with the norm: $\chi \circ N_{F_q^n/F_q} \in X(F_q^n)$. 

and in particular for the case $d = 2$,

$$\# \{ x \in F_q : x^2 = a \} = 1 + \mu_q(a).$$

(1.1.4)

For proofs of these identities see for instance Chapter 8.1 of [1].
Lemma 1.1.8. Take \( n, d \in \mathbb{Z}_{\geq 1} \) with \( d \mid q - 1 \). For all \( \chi \in X \left( \mathbb{F}_q^* \right) \) with order dividing \( d \), the lifted character \( \chi \circ N_{\mathbb{F}_{q^n}/\mathbb{F}_q} \in X \left( \mathbb{F}_{q^n}^* \right) \) also has order dividing \( d \). Furthermore, the map

\[
\varphi : \left\{ \chi \in X \left( \mathbb{F}_q^* \right) : \chi^d = \epsilon \right\} \to \left\{ \chi \in X \left( \mathbb{F}_{q^n}^* \right) : \chi^d = \epsilon \right\} \\
\chi \mapsto \chi \circ N_{\mathbb{F}_{q^n}/\mathbb{F}_q}
\]

is a bijection.

Proof. Consider \( \chi \in X \left( \mathbb{F}_q^* \right) \) with \( \chi^d = \epsilon \). Then for all \( a \in \mathbb{F}_{q^n}^* \),

\[
\chi \left( N_{\mathbb{F}_{q^n}/\mathbb{F}_q} (a) \right)^d = \epsilon \left( N_{\mathbb{F}_{q^n}/\mathbb{F}_q} (a) \right) = 1,
\]

and so \( \left( \chi \circ N_{\mathbb{F}_{q^n}/\mathbb{F}_q} \right)^d = \epsilon \).

Suppose \( \chi, \rho \in X \left( \mathbb{F}_q^* \right) \) are distinct. Then there exists \( a \in \mathbb{F}_q \) such that \( \chi (a) \neq \rho (a) \). Because the norm is surjective, there exists \( \alpha \in \mathbb{F}_{q^n}^* \) such that \( N_{\mathbb{F}_{q^n}/\mathbb{F}_q} (\alpha) = a \). Then \( \chi \left( N_{\mathbb{F}_{q^n}/\mathbb{F}_q} (\alpha) \right) \neq \rho \left( N_{\mathbb{F}_{q^n}/\mathbb{F}_q} (\alpha) \right) \). Thus \( \varphi \) is injective.

Note that \( \#X \left( \mathbb{F}_q^* \right) = q - 1 \) and \( \#X \left( \mathbb{F}_{q^n}^* \right) = q^n - 1 \). Because

\[
q^n - 1 = (q - 1) \left( q^{n-1} + q^{n-2} + \cdots + q + 1 \right),
\]

we have that \( d \mid q - 1 \mid q^n - 1 \). Hence, because \( X \left( \mathbb{F}_q^* \right) \) and \( X \left( \mathbb{F}_{q^n}^* \right) \) are cyclic, the number of elements of order dividing \( d \) in both groups is \( d \). Because \( \varphi \) is an injective map between finite sets of the same cardinality, we have that \( \varphi \) is also surjective. \( \square \)

1.2 Legendre Sums

Definition 1.2.1. For any \( b \in \mathbb{F}_q \) and \( \chi \in X \left( \mathbb{F}_q^* \right) \), the corresponding Legendre sum is the sum

\[
S_q (\chi; b) := \sum_{x \in \mathbb{F}_q} \chi (x) \mu_q (Q_b (x)),
\]

where \( Q_b = T^2 + 2bT + 1 \in \mathbb{F}_q [T] \).

Proposition 1.2.2. Take \( b \in \mathbb{F}_q \) and \( \chi \in X \left( \mathbb{F}_q^* \right) \). Then,

(a) \( S_q (\chi; b) \in \mathbb{R} \).

(b) \( S_q (\chi; \pm 1) = \begin{cases} q - 1, & \chi = \epsilon \\ 0, & \chi \neq \epsilon \end{cases} \).

(c) If \( b \neq \pm 1 \), then \( S_q (\epsilon, b) = -1 \).

Proof. (a) Note that for \( x \in \mathbb{F}_q^* \),

\[
\mu_q (Q_b (x^{-1})) = \mu_q \left( (x^{-1})^2 Q_b (x) \right) = \mu_q (Q_b (x)).
\]
Using this fact, the complex conjugate of \( S_q(\chi; b) \) is given by

\[
S_q^*(\chi; b) = \chi(0) \mu_q(Q_b(0)) + \sum_{x \in \mathbb{F}_q^*} \chi(x) \mu_q(Q_b(x))
\]

\[
= \chi(0) \mu_q(Q_b(0)) + \sum_{x \in \mathbb{F}_q^*} \chi(x^{-1}) \mu_q(Q_b(x^{-1}))
\]

\[
= S_q(\chi; b).
\]

(b) \[ S_q(\chi; \pm 1) = \sum_{x \in \mathbb{F}_q} \chi(x) \mu_q(Q_{\pm 1}(x)) = \sum_{x \in \mathbb{F}_q} \chi(x) \mu_q(x \pm 1)^2 \]

\[ = \sum_{x \in \mathbb{F}_q} \chi(x) = \begin{cases} q - 1, & \chi = \epsilon \\ 0, & \chi \neq \epsilon \end{cases} \]

(c) Let \( \Delta = b^2 - 1 \). Then, using (1.1.4), we have that

\[
S_q(\epsilon; b) = \sum_{x \in \mathbb{F}_q} \mu_q(Q_b(x)) = -q + \sum_{x \in \mathbb{F}_q} (1 + \mu_q((x + b)^2 - \Delta))
\]

\[ = -q + \sum_{x \in \mathbb{F}_q} (1 + \mu_q(x^2 - \Delta)) = -q + \sum_{x \in \mathbb{F}_q} \# \{ y \in \mathbb{F}_q : y^2 = x^2 - \Delta \}
\]

\[ = -q + \# \{ (x, y) \in \mathbb{F}_q^2 : (x + y)(x - y) = \Delta \} = -q + q - 1
\]

\[ = -1. \]

\[
\square
\]

2 The Hasse-Davenport Relation

In this section we prove what we will call the Hasse-Davenport relation for Legendre sums.

**Theorem 2.0.1** (Hasse-Davenport Relation for Legendre Sums). Consider nontrivial \( \chi \in X(\mathbb{F}_q^*) \) and \( b \in \mathbb{F}_q \setminus \{ \pm 1 \} \). There exist \( \alpha, \beta \in \mathbb{C} \) such that \( \alpha \beta = q \) and such that for all \( n \in \mathbb{Z}_{\geq 1} \),

\[ -S_{q^n}(\chi \circ N_{\mathbb{F}_{q^n}/\mathbb{F}_q}; b) = \alpha^n + \beta^n. \]

Here \( \alpha \) and \( \beta \) implicitly depend on \( \chi \) and \( b \), and we will throughout this paper fix \( b \) and write \( \alpha_\chi, \beta_\chi \) for the \( \alpha, \beta \) corresponding to a particular character \( \chi \).

We also prove the following.

**Theorem 2.0.2** (Riemann Hypothesis for Legendre Sums). The \( \alpha \) and \( \beta \) that arise in Theorem 2.0.1 have \( |\alpha| = |\beta| = \sqrt{q} \).

An immediate consequence of these theorems and Proposition 1.2.2 is the following.
Theorem 2.0.3. For $b \in \mathbb{F}_q \setminus \{\pm 1\}$ and $\chi \in X(\mathbb{F}_q^*)$, we have that $|S_q(\chi; b)| \leq 2\sqrt{q}$.

We break up the proof of Theorem 2.0.1 into two parts. First, we find $\alpha, \beta \in \mathbb{C}$ such that $\alpha \beta = q$ and $\alpha + \beta = -S_q(\chi; b)$. Then, we relate $\alpha^n$ and $\beta^n$ to $S_q^n(\chi \circ N_{\mathbb{F}_q^n/\mathbb{F}_q}; b)$. After proving Theorem 2.0.1, we show that $\alpha$ and $\beta$ have the desired magnitude.

2.1 Constructing $\alpha$ and $\beta$

Consider $b \in \mathbb{F}_q \setminus \{\pm 1\}$ and nontrivial $\chi \in X(\mathbb{F}_q^*)$. Let $z_1, z_2 \in \overline{\mathbb{F}}_q$ be the roots of $Q_b$. Writing $Q_b = (T - z_1)(T - z_2)$, we immediately obtain the relations $z_1 + z_2 = -2b$ and $z_1z_2 = 1$. Furthermore, because $b \neq \pm 1$, the discriminant $4(b^2 - 1)$ of $Q_b$ is nonzero, and $z_1$ and $z_2$ are distinct. Denote by $\mathbb{F}_q \lbrack T \rbrack$ the set of monic polynomials over $\mathbb{F}_q$. We define the map

$$\lambda : \mathbb{F}_q \lbrack T \rbrack \rightarrow \mathbb{C},$$

$$f \mapsto \chi \left( (-1)^{\deg f} f(0) \right) \mu_q(f(z_1)f(z_2)),$$

and we note that $\lambda$ is well-defined, since if we write $f = \sum_{i=1}^{\deg f} a_i T^i$, then

$$f(z_1)f(z_2) = \sum_{1 \leq i, j \leq \deg f} a_i a_j z_1^i z_2^j \leq \sum_{1 \leq i < j \leq \deg f} a_i a_j z_1^i z_2^j + \sum_{i=1}^{\deg f} a_i^2 (z_1 z_2)^i$$

$$= \sum_{1 \leq i < j \leq \deg f} a_i a_j z_1^j z_2^{-i} + \sum_{1 \leq i < j \leq \deg f} a_i a_j z_1^i z_2^{-j} + \sum_{i=1}^{\deg f} a_i^2$$

$$= \sum_{1 \leq i < j \leq \deg f} a_i a_j (-2b) + \sum_{i=1}^{\deg f} a_i^2 \in \mathbb{F}_q.$$

Furthermore, it is easy to see that $\lambda$ is multiplicative, i.e. that for two monic polynomials $f$ and $g$, $\lambda(fg) = \lambda(f) \lambda(g)$.

Lemma 2.1.1. For $k \in \mathbb{Z}_{\geq 0}$, let

$$\sigma(k) = \sum_{f \in \mathbb{F}_q \lbrack T \rbrack \atop \deg f = k} \lambda(f).$$

Then $\sigma(0) = 1$, $\sigma(1) = S_q(\chi; b)$, $\sigma(2) = q$, and $\sigma(k) = 0$ for $k \geq 3$.

Proof. There is exactly one monic polynomial of degree 0, namely 1, and furthermore $\lambda(1) = 1$. Hence $\sigma(0) = 1$. 

For polynomials of degree 1, we have:

$$\sigma(1) = \sum_{x \in \mathbb{F}_q} \lambda(T - x) = \sum_{x \in \mathbb{F}_q} \chi(x) \mu_q((z_1 - x)(z_2 - x))$$

$$= \sum_{x \in \mathbb{F}_q} \chi(x) \mu_q(Q_b(x)) = S_q(\chi; b).$$

For polynomials \( f \) of degree 2, we consider the Euclidean division \( f = Q_b + B \) of \( f \) by \( Q_b \), where \( \deg B < 2 \). Here the coefficient before the \( Q_b \) term is 1 because \( f \) and \( Q_b \) are monic of the same degree. This gives

$$\sigma(2) = \sum_{B \in \mathbb{F}_q[T], \deg B < 2} \lambda(Q_b + B) = \sum_{x, y \in \mathbb{F}_q} \lambda(Q_b + xT + y)$$

$$= \sum_{x, y \in \mathbb{F}_q} \chi(1 + y) \mu_q((xz_1 + y)(xz_2 + y))$$

$$= \sum_{x, y \in \mathbb{F}_q} \chi(1 + y) \mu_q(x^2 - 2bxy + y^2)$$

$$= \sum_{y \in \mathbb{F}_q} \chi(1 + y) \sum_{x \in \mathbb{F}_q} \mu_q((x - by)^2 - \Delta_y),$$

where \( \Delta_y = (b^2 - 1)y^2 \). Then, for \( y \in \mathbb{F}_q \),

$$\sum_{x \in \mathbb{F}_q} \mu_q((x - by)^2 - \Delta_y) = \sum_{a \in \mathbb{F}_q} \mu_q(a^2 - \Delta_y)$$

$$= -q + \sum_{a \in \mathbb{F}_q} (1 + \mu_q(a^2 - \Delta_y))$$

$$= -q + \sum_{a \in \mathbb{F}_q} \# \left\{ z \in \mathbb{F}_q : z^2 = a^2 - \Delta_y \right\}$$

$$= -q + \# \left\{ (a, z) \in \mathbb{F}_q^2 : \Delta_y = (a - z)(a + z) \right\}$$

$$= -q + \# \left\{ (u, v) \in \mathbb{F}_q^2 : \Delta_y = uv \right\}$$

$$= \begin{cases} -1 & \Delta_y \neq 0, \\ q - 1 & \Delta_y = 0. \end{cases}$$

Here we used (1.1.4) between the second and third lines. Because \( b \neq \pm 1 \), \( \Delta_y = 0 \) if and only if \( y = 0 \). This gives us,

$$\sigma(1) = \chi(1)(q - 1) - \sum_{y \in \mathbb{F}_q^*} \chi(1 + y) = q.$$
varies over all polynomials of degree at most 2. Hence, we may write

$$\sigma(k) = \sum_{f \in \mathbb{F}_q[T], \deg f = k} \lambda(f) = \sum_{A \in \mathbb{F}_q[T], \deg A = k-2} \sum_{B \in \mathbb{F}_q[T], \deg B < 2} \lambda(AQ_b + B)$$

$$= \sum_{x_0, x_2, \ldots, x_{k-3} \in \mathbb{F}_q} \lambda\left(\sum_{i=0}^{k-3} x_i T^i\right) Q_b + (y_1 T + y_0)$$

$$= \sum_{x_0, x_2, \ldots, x_{k-3} \in \mathbb{F}_q} \chi\left((-1)^k (x_0 + y_0)\right) \mu_q \left(\left(y_1 z_1 + y_0\right) \left(y_1 z_2 + y_0\right)\right) \sum_{x_0 \in \mathbb{F}_q} \chi(x_0 + y_0),$$

and by (1.1.2), \(\sum_{x \in \mathbb{F}_q} \chi(x + y_2) = 0\), since \(\chi\) is nontrivial. \(\square\)

Now define the formal power series

$$L(z) := \sum_{f \in \mathbb{F}_q[T]} \lambda(f) z^{\deg f}. \quad (2.1.2)$$

By the previous lemma, we see that \(L(z)\) is actually a quadratic polynomial. Namely,

$$L(z) = \sum_{k=1}^{\infty} \sigma(k) z^k = 1 + S_q(\chi; b) z + qz^2 = (1 - \alpha z)(1 - \beta z), \quad (2.1.3)$$

for some \(\alpha, \beta \in \mathbb{C}\). Furthermore, \(\alpha \beta = q\) and \(\alpha + \beta = -S_q(\chi; b)\). We thus have constructed the \(\alpha\) and \(\beta\) that we wanted.

### 2.2 Taking Powers of \(\alpha\) and \(\beta\)

**Lemma 2.2.1.** Let \(L(z)\) be as in (2.1.2). We have that

$$L(z) = \prod_{f \in \mathbb{F}_q[T], \text{irreducible}} \frac{1}{1 - \lambda(f) z^{\deg f}}.$$

**Proof.** Because \(\mathbb{F}_q[T]\), of which \(\mathbb{F}_q^m[T]\) is a subset, is a unique factorization domain whose prime elements are the irreducible polynomials, we may write

$$L(z) = \sum_{f \in \mathbb{F}_q[T]} \lambda(f) z^{\deg f} = \prod_{f \in \mathbb{F}_q[T], \text{irreducible}} \sum_{k=1}^{\infty} \lambda(f^k) z^{k \deg f^k}$$

$$= \prod_{f \in \mathbb{F}_q[T], \text{irreducible}} \sum_{k=1}^{\infty} \lambda(f)^k z^{k \deg f} = \prod_{f \in \mathbb{F}_q[T], \text{irreducible}} \frac{1}{1 - \lambda(f) z^{\deg f}},$$

where in the last step we used the fact that the summation is a geometric series. \(\square\)
Lemma 2.2.2. For all \( n \in \mathbb{Z}_{\geq 1} \),

\[
\alpha^n + \beta^n = \sum_{\substack{f \in \mathbb{F}_q[T] \\
\text{irreducible} \\
\deg f \mid n}} \lambda(f)^{n/\deg f} \deg f.
\]

Proof. By (2.1.3) and Lemma 2.2.1,

\[
(1 - \alpha z)(1 - \beta z) = \prod_{f \in \mathbb{F}_q[T] \atop \text{irreducible}} \frac{1}{1 - \lambda(f) z^{\deg f}}.
\]

Taking the logarithmic derivative of both sides and multiplying by \(-z\) gives

\[
\frac{\alpha z}{1 - \alpha z} + \frac{\beta z}{1 - \beta z} = -\sum_{f \in \mathbb{F}_q[T] \atop \text{irreducible}} \frac{\lambda(f) (\deg f) z^{\deg f}}{1 - \lambda(f) z^{\deg f}}.
\]

Expanding the left side in geometric series gives

\[
\frac{\alpha z}{1 - \alpha z} + \frac{\beta z}{1 - \beta z} = \sum_{n=1}^{\infty} (\alpha^n + \beta^n) z^n.
\]

Expanding the right side gives

\[
-\sum_{f \in \mathbb{F}_q[T] \atop \text{irreducible}} \frac{\lambda(f) (\deg f) z^{\deg f}}{1 - \lambda(f) z^{\deg f}} = -\sum_{f \in \mathbb{F}_q[T] \atop \text{irreducible}} \lambda(f) (\deg f) z^{\deg f} \sum_{k=0}^{\infty} \lambda(f)^k z^{k \deg f}
\]

\[
= -\sum_{k=1}^{\infty} \sum_{f \in \mathbb{F}_q[T] \atop \text{irreducible}} \lambda(f)^k (\deg f) z^{k \deg f}.
\]

Substituting \( n = k \deg f \), we obtain

\[
-\sum_{k=1}^{\infty} \sum_{f \in \mathbb{F}_q[T] \atop \text{irreducible}} \lambda(f)^k (\deg f) z^{k \deg f} = -\sum_{n=1}^{\infty} \sum_{f \in \mathbb{F}_q[T] \atop \text{irreducible} \atop \deg f \mid n} \lambda(f)^{n/\deg f} (\deg f) z^n
\]

We thus have that

\[
\sum_{n=1}^{\infty} (\alpha^n + \beta^n) z^n = -\sum_{n=1}^{\infty} \sum_{f \in \mathbb{F}_q[T] \atop \text{irreducible} \atop \deg f \mid n} \lambda(f)^{n/\deg f} (\deg f) z^n.
\]

Equating like coefficients gives the desired result. \(\square\)
Lemma 2.2.3. Consider \( n \in \mathbb{Z}_{\geq 1} \) and irreducible \( f \in \mathbb{F}_q^m[T] \) such that \( \deg f \mid n \). Then for all roots \( \zeta \in \mathbb{F}_q \) of \( f \),

\[
\lambda(f)^{n/\deg f} = (\chi \circ N_{\mathbb{F}_q^n/\mathbb{F}_q})(\zeta) \mu_{q^n}(Q_b(\zeta)).
\]

Proof. Because \( f \) is monic and irreducible, \( f \) is the minimum polynomial of \( \zeta \), and the roots of \( f \) are \( \zeta, \zeta^q, \zeta^{q^2}, \ldots, \zeta^{\deg f - 1} \) (see for instance Chapter 6.2 of [2]). We have that

\[
\lambda(f)^{n/\deg f} = \chi((-1)^{\deg f} f(0))^{n/\deg f} \mu_q(f(z_1) f(z_2))^{n/\deg f}.
\]

For the \( \chi \) term,

\[
\chi((-1)^{\deg f} f(0))^{n/\deg f} = \chi((-1)^{\deg f} (-1)^{\deg f} \prod_{k=0}^{\deg f - 1} \zeta^{q^k})^{n/\deg f} = \left(\chi \circ N_{\mathbb{F}_{q^\deg f}/\mathbb{F}_q}\right)(\zeta)^{n/\deg f} = \left(\chi \circ N_{\mathbb{F}_q^n/\mathbb{F}_q}\right)(\zeta).
\]

For the \( \mu_q \) term,

\[
\mu_q(f(z_1) f(z_2))^{n/\deg f} = \mu_q \left( \prod_{k=0}^{\deg f - 1} \left( z_1 - \zeta^{q^k} \right) \left( z_2 - \zeta^{q^k} \right) \right)^{n/\deg f} = \mu_q \left( \prod_{k=0}^{\deg f - 1} Q_b(\zeta)^{q^k} \right)^{n/\deg f} = \left(\mu_q \circ N_{\mathbb{F}_{q^\deg f}/\mathbb{F}_q}\right)(Q_b(\zeta))^{n/\deg f} = \mu_{q^n}(Q_b(\zeta)).
\]

This gives the desired result.

Applying Lemmas 2.2.2 and 2.2.3 now completes the proof of Theorem 2.0.1:

\[
-S_{q^n}(\chi \circ N_{\mathbb{F}_q^n/\mathbb{F}_q}; b) = - \sum_{\zeta \in \mathbb{F}_q^n} \left( \chi \circ N_{\mathbb{F}_q^n/\mathbb{F}_q}(\zeta) \mu_{q^n}(Q_b(\zeta)) \right) = - \sum_{f \in \mathbb{F}_q^m[T]} \sum_{\substack{\zeta \in \mathbb{F}_q^n \\ \text{irreducible} \ f(\zeta) = 0}} \left( \chi \circ N_{\mathbb{F}_q^n/\mathbb{F}_q}(\zeta) \mu_{q^n}(Q_b(\zeta)) \right) = - \sum_{f \in \mathbb{F}_q^m[T]} \sum_{\substack{\text{irreducible} \ f(\zeta) = 0 \ f \mid n}} \lambda(f)^{n/\deg f} \deg f = \alpha^n + \beta^n.
\]
2.3 The Magnitude of $\alpha$ and $\beta$

In order to show that $|\alpha| = |\beta| = \sqrt{q}$, we construct a smooth projective algebraic curve whose zeta function has among its roots $\alpha^{-1}$ and $\beta^{-1}$, and then we apply the Riemann hypothesis for curves over finite fields. See Chapter 4 and in particular Theorem 4.2.3 of [3] for more information on the zeta function of a curve and the corresponding Riemann hypothesis.

Consider the polynomial $f = Y^2 - Q_b \left(X^d\right) \in \mathbb{F}_q [X, Y]$ for $d \mid q - 1$. Then $f$ is irreducible in $\mathbb{F}_q [X, Y]$, since $b \neq \pm 1$ implies that $Q_b \left(X^d\right)$ is not a square in $\mathbb{F}_q [X]$. Let $C_0$ be the affine variety over $\mathbb{F}_q$ defined by $f (x, y) = 0$. We have that

$$\frac{\partial f (x, y)}{\partial x} = 2dx^d \left(-x^{d-1} + b\right) \quad \text{and} \quad \frac{\partial f (x, y)}{\partial y} = 2y$$

both vanish only at $(x, y) = (0, 0)$ and $(x, y) = \left(d^{-\frac{1}{2}}b, 0\right)$, since $d$ and $q$ are coprime. Because $(0, 0), \left(d^{-\frac{1}{2}}b, 0\right) \notin C_0$, $C_0$ has no singular points and is thus smooth. We now count the number of $\mathbb{F}_{q^n}$-rational points of $C_0$ for all $n \in \mathbb{Z}_{\geq 1}$. Applying (1.1.3), we have that

$$\#C_0 (\mathbb{F}_{q^n}) = \# \{ (x, y) \in \mathbb{F}_{q^n}^2 : y^2 = Q_b \left(x^d\right) \} = \sum_{x \in \mathbb{F}_{q^n}} \# \{ y \in \mathbb{F}_{q^n} : y^2 = Q_b \left(x^d\right) \}$$

$$= \sum_{x \in \mathbb{F}_{q^n}} (1 + \mu_{q^n} (Q_b \left(x^d\right))) = q^n + \sum_{x \in \mathbb{F}_{q^n}} \# \{ x \in \mathbb{F}_{q^n} : z = x^d \} \mu_{q^n} (Q_b (z))$$

$$= q^n + \sum_{x \in \mathbb{F}_{q^n}} \sum_{\chi \in X (\mathbb{F}_{q^n})} \chi (z) \mu_{q^n} (Q_b (z)) = q^n + \sum_{\chi \in X (\mathbb{F}_{q^n})} S_{q^n} (\chi; b).$$

By Proposition 1.2.2, $S_{q^n} (\epsilon; b) = -1$, and hence

$$\#C_0 (\mathbb{F}_{q^n}) = q^n - 1 + \sum_{\chi \in X (\mathbb{F}_{q^n})} S_{q^n} (\chi; b).$$

By Lemma 1.1.8,

$$\sum_{\chi \in X (\mathbb{F}_{q^n})} S_{q^n} (\chi; b) = \sum_{\chi \in X (\mathbb{F}_{q^n})} S_{q^n} (\chi \circ N_{\mathbb{F}_{q^n} / \mathbb{F}_q}; b).$$

For all nontrivial $\chi \in X (\mathbb{F}_q^*)$ we can take $\alpha_{\chi}, \beta_{\chi} \in \mathbb{C}$ as in Theorem 2.0.1. Then,

$$\#C_0 (\mathbb{F}_{q^n}) = q^n - 1 - \sum_{\chi \in X (\mathbb{F}_{q^n})} \left(\alpha^n_{\chi} + \beta^n_{\chi}\right).$$
The projective closure $\widetilde{C}_0$ of $C_0$ is the set of solutions $[x : y : z] \in \mathbb{P}^2(\mathbb{F}_q)$ to the polynomial equation $\tilde{f}(x, y, z) = 0$ where $\tilde{f}(x, y, z) = y^2z^{2(d-1)} - x^{2d} - 2bx^d z^d - z^{2d}$. The points at infinity of $\widetilde{C}_0$ are then points on $\widetilde{C}_0 \cap \{z = 0\}$, i.e. the single solution $[0 : 1 : 0]$ to the equation $x^{2d} = 0$. Unfortunately, this point is singular, so we cannot apply the Riemann hypothesis for curves over finite fields to $\widetilde{C}_0$.

In order to rectify this problem, we first define the affine variety $C$ to be the set of points $(\mu_1, \mu_2, \ldots, \mu_d, \mu_{d+1}) \in \mathbb{A}^{d+1}(\mathbb{F}_q)$ satisfying

$$
\mu_2 = \mu_1^2, \quad \mu_1 \mu_3 = \mu_2^2, \quad \ldots, \quad \mu_{d-2} \mu_d = \mu_{d-1}^2, \quad \text{and} \quad \mu_{d+1}^2 = Q_b(\mu_d).
$$

Then for all $1 \leq i \leq d$, $\mu_i = \mu_1^i$, and we can see that $C$ is isomorphic to $C_0$, e.g. by the polynomial map $(u_1, \ldots, u_{d+1}) \mapsto (u_1, u_{d+1})$ and its inverse $(u, v) \mapsto (u, u^2, u^3, \ldots, u^d, v)$. Hence $\#C(\mathbb{F}_q^n) = \#C_0(\mathbb{F}_q^n)$ for all $n \in \mathbb{Z}_{\geq 1}$. The projective closure of $C$ is the projective curve $\widetilde{C} \subseteq \mathbb{P}^{d+1}$ defined by the $2d - 2$ polynomial equations

$$
F_1 : \mu_1^2 - \mu_0 \mu_2 = 0, \quad G_0 : \mu_0 \mu_d - \mu_1 \mu_{d-1} = 0,
\quad F_2 : \mu_2^2 - \mu_1 \mu_3 = 0, \quad G_1 : \mu_1 \mu_d - \mu_2 \mu_{d-1} = 0,
\vdots
\quad F_{d-2} : \mu_{d-2}^2 - \mu_{d-3} \mu_{d-1} = 0, \quad G_{d-3} : \mu_{d-3} \mu_d - \mu_{d-2} \mu_{d-1} = 0,
\quad F_{d-1} : \mu_{d-1}^2 - \mu_{d-2} \mu_d = 0, \quad H : \mu_{d+1}^2 - \mu_d^2 - 2b \mu_0 \mu_d - \mu_0^2 = 0.
$$

The points at infinity are the points on $\widetilde{C} \cap \{\mu_0 = 0\}$. This gives two points at infinity, namely the points $[0 : \ldots : 0 : \pm 1 : 1]$, both of which are $\mathbb{F}_q$-rational. To show that these points are nonsingular, we consider the affine part $\widetilde{C} \cap \{\mu_{d+1} = 1\}$ of $\widetilde{C}$ containing both points at infinity. Its Jacobian matrix is the $(2d - 2) \times (d + 1)$ matrix

$$
\begin{pmatrix}
-\mu_2 & 2\mu_1 & -\mu_0 & 0 & \cdots & 0 & 0 & 0 & 0 \\
0 & -\mu_3 & 2\mu_2 & -\mu_1 & \cdots & 0 & 0 & 0 & 0 \\
0 & 0 & -\mu_4 & 2\mu_3 & \cdots & 0 & 0 & 0 & 0 \\
\vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots \\
\vdots & \vdots & \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots \\
0 & 0 & 0 & 0 & \cdots & -\mu_{d-1} & 2\mu_{d-2} & -\mu_{d-3} & 0 \\
0 & 0 & 0 & 0 & \cdots & 0 & -\mu_d & 2\mu_{d-1} & -\mu_{d-2} \\
\mu_d & -\mu_{d-1} & 0 & 0 & \cdots & 0 & 0 & -\mu_1 & \mu_0 \\
0 & \mu_d & -\mu_{d-1} & 0 & \cdots & 0 & 0 & -\mu_2 & \mu_1 \\
0 & 0 & \mu_d & -\mu_{d-1} & \cdots & 0 & 0 & -\mu_3 & \mu_2 \\
\vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots \\
\vdots & \vdots & \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots \\
0 & 0 & 0 & 0 & \cdots & \mu_d & -\mu_{d-1} & -\mu_{d-1} & \mu_{d-2} \\
2b \mu_d & + 2\mu_0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 2\mu_d + 2b \mu_0
\end{pmatrix},
$$

where the rows are ordered $F_1, F_2, \ldots, F_{d-1}, G_0, G_1, \ldots, G_{d-3}, H$. Evaluated at the
points at infinity, this becomes the matrix

\[
\begin{pmatrix}
0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\
\vdots & \ddots & \ddots & \ddots & \cdots & \ddots & \ddots & \ddots \\
\vdots & \ddots & \ddots & \ddots & \cdots & \ddots & \ddots & \ddots \\
0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\
\pm 1 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\
0 & \pm 1 & 0 & 0 & \cdots & 0 & 0 & 0 \\
0 & 0 & \pm 1 & 0 & \cdots & 0 & 0 & 0 \\
\vdots & \ddots & \ddots & \ddots & \cdots & \ddots & \ddots & \ddots \\
\vdots & \ddots & \ddots & \ddots & \cdots & \ddots & \ddots & \ddots \\
0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\
\pm 2b & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\
\end{pmatrix},
\]

which has rank \(d\). Thus the dimension of the tangent spaces at the points at infinity is \(\dim A^{d+1} - d = (d+1) - d = 1\), and the points at infinity are nonsingular. Hence \(\tilde{C}\) is smooth, and furthermore \(\#\tilde{C}(\mathbb{F}_{q^n}) = 2 + C_0(\mathbb{F}_{q^n})\) for all \(n \in \mathbb{Z}_{\geq 1}\).

We now calculate the zeta function for \(\tilde{C}\):

\[
\log Z\left(\tilde{C}/\mathbb{F}_q; T\right) = \sum_{n=1}^{\infty} \frac{\#\tilde{C}(\mathbb{F}_{q^n})}{n} T^n
= \sum_{n=1}^{\infty} \frac{q^n + 1}{n} T^n - \sum_{\chi \in \chi^d \neq \epsilon} \sum_{n=1}^{\infty} \frac{\alpha_n^\chi + \beta_n^\chi}{n} T^n
= \sum_{\chi \in \chi^d \neq \epsilon} \log \left(1 - \alpha_\chi T \right) \left(1 - \beta_\chi T \right) - \log (1 - T) - \log (1 - qT),
\]

and so

\[
Z\left(\tilde{C}/\mathbb{F}_q; T\right) = \prod_{\chi \in \chi^d \neq \epsilon} \frac{(1 - \alpha_\chi T)(1 - \beta_\chi T)}{(1 - T)(1 - qT)} .
\]

By the Riemann hypothesis for curves over finite fields, the inverses of the roots of \(Z\left(\tilde{C}/\mathbb{F}_q; T\right)\) have magnitude \(\sqrt{q}\). If we choose \(d = q - 1\), then the product is over all nontrivial multiplicative characters on \(\mathbb{F}_q\), and we have completed the proof of Theorem 2.0.2.
3 Equidistribution Theorems

Take $b \in \mathbb{F} \setminus \{\pm 1\}$. By Theorem 2.0.1, for all nontrivial $\chi \in X (\mathbb{F}^*_q)$,

$$|S_q (\chi; b)| = |\alpha_\chi + \beta_\chi| \leq 2 \sqrt{q},$$

for some $\alpha_\chi, \beta_\chi \in \mathbb{C}$ with $\alpha_\chi \beta_\chi = q$. Because $S_q (\chi; b)$ is a real number we obtain a unique angle $\theta_\chi \in [0, \pi]$ from the equation

$$S_q (\chi; b) = 2 \sqrt{q} \cos (\theta_\chi). \quad (3.0.1)$$

Equivalently,

$$\{\alpha_\chi, \beta_\chi\} = \{-\sqrt{q} \exp (i \theta_\chi), -\sqrt{q} \exp (-i \theta_\chi)\}. \quad (3.0.2)$$

3.1 Character Sums

Let $p$ be the characteristic of $\mathbb{F}_q$, and let $\psi : \mathbb{F}_q \to \mathbb{C}$ be the additive character given by $\psi (x) = \exp \left( \frac{2 \pi i}{p} \Tr_{\mathbb{F}_q/\mathbb{F}_p} (x) \right)$. For multiplicative characters $\chi, \rho \in X (\mathbb{F}_q^*)$, denote by $G (\chi)$ and $J (\chi, \rho)$ the respective Gauss and Jacobi sums:

$$G (\chi) = \sum_{x \in \mathbb{F}_q} \chi (x) \psi (x),$$
$$J (\chi, \rho) = \sum_{x \in \mathbb{F}_q} \chi (x) \rho (1 - x) = \sum_{x \in \mathbb{F}_q} \chi (1 - x) \rho (x).$$

Recall the following properties of Gauss and Jacobi sums.

**Proposition 3.1.1.** We have that

$$G (\epsilon) = 0.$$

Let $\chi \in X (\mathbb{F}_q^*)$ be a nontrivial multiplicative character. Then,

$$|G (\chi)| = \sqrt{q},$$
$$G (\chi) G (\overline{\chi}) = \chi (-1) q.$$

In particular for the case $\chi = \mu_q$,

$$\mu_q (-1) G (\mu_q)^2 = q.$$

**Proposition 3.1.2.** If $\chi, \rho \in X (\mathbb{F}_q^*)$ are such that $\chi, \rho$, and $\chi \rho$ are all nontrivial, then

$$|J (\chi, \rho)| = \sqrt{q},$$
$$J (\chi, \rho) = \frac{G (\chi) G (\rho)}{G (\chi \rho)}. $$

17
See Chapters 8.2 and 8.3 of [1] for proofs of these properties.

Consider collections \( (\chi_i)_{i=1}^m \) and \( (\rho_j)_{j=1}^n \) of multiplicative characters on \( \mathbb{F}_q \), and consider \( t \in \mathbb{F}_q^* \). In [4], Katz defines the hypergeometric sum corresponding to this data to be the sum

\[
\text{Hyp}_{m,n} \left( \psi, (\chi_i)_{i=1}^m, (\rho_j)_{j=1}^n \right) (\mathbb{F}_q, t) := \sum_{\substack{x_1, \ldots, x_m, y_1, \ldots, y_n \in \mathbb{F}_q \\ \prod_{i=1}^m x_i = t \prod_{j=1}^n y_j}} \psi \left( \sum_{i=1}^m x_i - \sum_{j=1}^n y_j \right) \left( \prod_{i=1}^m \chi_i(x_i) \right) \left( \prod_{j=1}^n \rho_j(y_j) \right).
\]

**Lemma 3.1.3.** Suppose that \( \{\chi_i : 1 \leq i \leq m\} \cap \{\rho_j : 1 \leq j \leq n\} = \emptyset \). Then we have the bound

\[
| \text{Hyp}_{m,n} \left( \psi, (\chi_i)_{i=1}^m, (\rho_j)_{j=1}^n \right) (\mathbb{F}_q, t) | \leq Rq^{w/2},
\]

where \( w = m + n - 1 \) and \( R = \max \{m, n\} \).

We do not prove this here. See [4] for a full discussion of hypergeometric sums and their corresponding hypergeometric sheaves. In particular, this bound is a consequence of Deligne’s proof of the Riemann hypothesis for varieties in [5], along with Katz’s construction. Note that in the case \( t = 1, m = 0 \), and \( \chi_i = \epsilon \) for \( i = 1, 2, \ldots, n \), the hypergeometric sums reduce to the well-known hyper-Kloosterman sums which satisfy the bound

\[
\left| \sum_{x_1, \ldots, x_n \in \mathbb{F}_q \atop \prod_{i=1}^n x_i = 1} \psi \left( \sum_{i=1}^n x_i \right) \right| \leq nq^{(n-1)/2}
\]

(see for instance Theorem 6 of [6]).

### 3.2 The Case \( b = 0 \)

**Proposition 3.2.1.** For all odd prime powers \( q \) and all \( \chi \in X (\mathbb{F}_q^*) \), we have that

\[
S_q (\chi; 0) = \begin{cases} 
0, & \chi \text{ non-square} \\
\eta(-1) J (\eta, \mu_q) + \mu_q \eta (-1) J (\mu_q \eta, \mu_q), & \chi = \eta^2
\end{cases}
\]

**Proof.** Suppose \( \chi \) is non-square. Then \( \chi (-1) = -1 \) by Proposition 1.1.5, and

\[
S_q (\chi; 0) = \sum_{x \in \mathbb{F}_q} \chi (x) \mu_q (x^2 + 1) = - \sum_{x \in \mathbb{F}_q} \chi (-x) \mu_q ((-x)^2 + 1) = -S_q (\chi; 0),
\]

so \( S_q (\chi; 0) = 0 \).
Suppose \( \chi = \eta^2 \) for some \( \eta \in X(\mathbb{F}_q^*) \). Then, using (1.1.4), we have that

\[
S_q(\chi; 0) = \sum_{x \in \mathbb{F}_q} \eta(x^2) \mu_q(x^2 + 1) = \sum_{y \in \mathbb{F}_q} \eta(y) \mu_q(y + 1) \# \{ x \in \mathbb{F}_q : x^2 = y \}
\]

\[
= \sum_{y \in \mathbb{F}_q} \eta(y) \mu_q(y + 1) + \sum_{y \in \mathbb{F}_q} \eta(y) \mu_q(y + 1) \mu_q(y)
\]

\[
= \sum_{y \in \mathbb{F}_q} \eta(-y) \mu_q(1 - y) + \sum_{y \in \mathbb{F}_q} \mu_q \eta(-y) \mu_q(1 - y)
\]

\[
= \eta(-1) J(\overline{\eta}, \mu_q) + \mu_q \eta(-1) J(\mu_q \overline{\eta}, \mu_q),
\]

where between the second and third lines we made the substitution \( y \to -y \). \( \square \)

We require the following equidistribution result for Jacobi sums.

**Proposition 3.2.2.** Write \( Y(\mathbb{F}_q^*) = X(\mathbb{F}_q^*) \setminus \{ \epsilon, \mu_q \} \) for all prime powers \( q \). Let \( \{ q_m \}_{m \geq 1} \) be a sequence of odd prime powers which tends to infinity. For \( \eta \in Y(\mathbb{F}_q^*) \), let \( \phi \in [0, 2\pi) \) be such that \( \eta(-1) J(\eta, \mu_q) = \sqrt{q} \exp(i\phi_{\eta}) \). Then the numbers \( \{ \phi_{\eta} \}_{\eta \in Y(\mathbb{F}_q^*)} \) become equidistributed with respect to the Haar measure, i.e., for all continuous maps \( f : [0, 2\pi] \to \mathbb{R} \), we have that

\[
\lim_{m \to \infty} \frac{1}{q_m - 3} \sum_{\eta \in Y(\mathbb{F}_q^*)} f(\phi_{\eta}) = \frac{1}{2\pi} \int_0^{2\pi} f(\phi) \, d\phi.
\]

(3.2.3)

**Proof.** Denote by \( C([0, \pi]) \) the Banach algebra of continuous real-valued functions on \([0, \pi]\) equipped with the supremum norm. By the Stone-Weierstrass theorem (see for instance Theorem 8.15 of [7]), the trigonometric polynomials are dense in \( C([0, \pi]) \). Because each trigonometric polynomial can be written as a linear combination of the maps \( \theta \mapsto \cos(n\theta), \ n \geq 0 \), it suffices to prove (3.2.3) for \( f \) equal to those maps. The case \( n = 0 \) is trivial, so consider \( n \geq 1 \). Then a simple computation shows that

\[
\frac{1}{2\pi} \int_0^{2\pi} \cos(n\phi) \, d\phi = 0,
\]

and that for \( \eta \in Y(\mathbb{F}_q^*) \),

\[
\cos(n\phi_{\eta}) = \text{Re} \left( \frac{\eta(-1) J(\eta, \mu_q)}{\sqrt{q}} \right)^n.
\]

We note that \( \sum_{\eta \in Y(\mathbb{F}_q^*)} (\eta(-1) J(\eta, \mu_q))^n \) is real, since

\[
\sum_{\eta \in Y(\mathbb{F}_q^*)} (\eta(-1) J(\eta, \mu_q))^n = \sum_{\eta \in Y(\mathbb{F}_q^*)} \left( \mu_q \eta(-1) \sum_{x \in \mathbb{F}_q} \mu_q \eta(x) \mu_q(1 - x) \right)^n
\]

\[
= \sum_{\eta' \in Y(\mathbb{F}_q^*)} (\eta'(-1) J(\eta', \mu_q))^n.
\]
Hence, we need to show that
\[ \lim_{m \to \infty} M_n(q_m) = 0 \]
for all \( n \geq 1 \), where
\[
M_n(q) := \frac{1}{q - 3} \sum_{\eta \in Y(F_q^*)} \left( \frac{\eta(-1)J(\eta, \mu_q)}{\sqrt{q}} \right)^n
\]
denotes the \( n \)-th normalized moment of the character sum given by \( \eta(-1)J(\eta, \mu_q) \) for \( \eta \in Y(F_q^*) \) over the field \( F_q \). Fix some \( q = q_m \). For \( \eta \in Y(F_q^*) \) we can write \( J(\eta, \mu_q) \) as a product of Gauss sums by applying Proposition 3.1.2 as follows:
\[
J(\eta, \mu_q) = \frac{1}{q} G(\eta) G(\mu_q) G(\mu_q \eta) \frac{\mu_q \eta(-1)}{\sqrt{q}} G(\eta) G(\mu_q) G(\mu_q \eta) .
\]
Then,
\[
M_n(q) = \frac{1}{q - 3} \left( \frac{\mu_q(-1)G(\mu_q)}{\sqrt{q}} \right)^n \sum_{\eta \in Y(F_q^*)} \left( \frac{G(\eta) G(\mu_q \eta)}{q} \right)^n ,
\]
where \( \mu_q(-1)G(\mu_q)/\sqrt{q} \) has magnitude 1. Because \( G(\epsilon) = 0 \), we have that
\[
\sum_{\eta \in Y(F_q^*)} (G(\eta) G(\mu_q \eta))^n = \sum_{\eta \in X(F_q^*)} (G(\eta) G(\mu_q \eta))^n - 2G(\epsilon)^n G(\mu_q)^n
\]
\[
= \sum_{\eta \in X(F_q^*)} (G(\eta) G(\mu_q \eta))^n ,
\]
and so
\[
|M_n(q)| \leq \frac{1}{q - 3} \left| \sum_{\eta \in X(F_q^*)} \left( \frac{G(\eta) G(\mu_q \eta)}{q} \right)^n \right| . \quad (3.2.4)
\]
Expanding each Gauss sum gives
\[
\sum_{\eta \in X(F_q^*)} (G(\eta) G(\mu_q \eta))^n = \sum_{\eta \in X(F_q^*)} \left( \sum_{y_1, \ldots, y_n \in F_q^*} \eta \left( \prod_{i=1}^n y_i \right) \psi \left( \prod_{i=1}^n y_i \right) \right) \cdot \left( \sum_{z_1, \ldots, z_n \in F_q^*} \mu_q \eta \left( \prod_{i=1}^n z_i \right) \psi \left( \prod_{i=1}^n z_i \right) \right) .
\]
Exchanging sums, we see that this equals
\[
\sum_{y_1, \ldots, y_n \in F_q^*} \psi \left( \sum_{i=1}^n (y_i + z_i) \right) \mu_q \left( \prod_{i=1}^n z_i \right) \sum_{\eta \in X(F_q^*)} \eta \left( \prod_{i=1}^n y_i / \prod_{i=1}^n z_i \right) .
\]
By (1.1.1), the rightmost term satisfies
\[
\sum_{\eta \in X(F_q^*)} \eta \left( \prod_{i=1}^{n} y_i / \prod_{i=1}^{n} z_i \right) = \begin{cases} 
q - 1, & \prod_{i=1}^{n} y_i = \prod_{i=1}^{n} z_i, \\
0, & \text{otherwise}
\end{cases}
\]

Hence,
\[
\sum_{\eta \in X(F_q^*)} (G(\eta) G(\mu_q \eta))^n
= (q - 1) \sum_{\substack{y_1, \ldots, y_n \in F_q \\
\Pi_{i=1}^{n} y_i = \prod_{i=1}^{n} z_i}} \psi \left( \sum_{i=1}^{n} (y_i + z_i) \right) \mu_q \left( \prod_{i=1}^{n} z_i \right).
\]

Substituting \( z_i \to -z_i \), this equals
\[
(q - 1) \mu_q \left( (-1)^n \right) \sum_{\substack{y_1, \ldots, y_n \in F_q \\
\Pi_{i=1}^{n} y_i = \prod_{i=1}^{n} z_i}} \psi \left( \sum_{i=1}^{n} (y_i - z_i) \right) \mu_q \left( \prod_{i=1}^{n} z_i \right).
\]

Contained in this expression is the hypergeometric sum
\[
\text{Hyp}_{n,n} \left( \psi, (\epsilon)_{i=1}^{n}, (\mu_q)_{i=1}^{n} \right) (F_q, (-1)^n)
= \sum_{\substack{y_1, \ldots, y_n \in F_q \\
\Pi_{i=1}^{n} y_i = \prod_{i=1}^{n} z_i}} \psi \left( \sum_{i=1}^{n} (y_i - z_i) \right) \mu_q \left( \prod_{i=1}^{n} z_i \right).
\]

Combining Lemma 3.1.3 with (3.2.4), we get that
\[
|\mathcal{M}_n(q)| \leq \frac{n(q - 1)}{\sqrt{q(q - 3)}},
\]
and so we can see that
\[
\lim_{m \to \infty} \mathcal{M}_n(q_m) = 0.
\]

\[\square\]

**Theorem 3.2.5** (Restatement of Theorem 0.0.1). Let \( \{q_m\}_{m \geq 1} \) be a sequence of odd prime powers which tends to infinity. For a given \( m \) and all \( \chi \in X(F_{q_m}^*) \) let \( \theta_\chi \) be the angle associated to the Legendre sum \( S_{q_m}(\chi; 0) \). Then the numbers \( \{\theta_\chi\}_{\chi \in X(F_{q_m}^*)} \) become equidistributed with respect to the measure which is the average of the Haar measure on \([0, \pi]\) and the Dirac delta measure at \( \pi/2 \) as \( m \to \infty \), i.e. for all continuous maps \( f : [0, \pi] \to \mathbb{R} \),
\[
\lim_{m \to \infty} \frac{1}{q_m - 1} \sum_{\chi \in X(F_{q_m}^*)} f(\theta_\chi) = \frac{1}{2\pi} \int_{0}^{\pi} f(\theta) \, d\theta + \frac{1}{2} f\left( \frac{\pi}{2} \right).
\] (3.2.6)
Proof. Just as in the proof of Proposition 3.2.2, it suffices to prove (3.2.6) for \( f(\theta) = \cos(n\theta), n \geq 0 \). The case \( n = 0 \) is straightforward:

\[
\lim_{m \to \infty} \frac{1}{q_m - 1} \sum_{\chi \in \chi(q_m)} \frac{1}{2\pi} \int_{0}^{\pi} \cos(n\theta) d\theta + \frac{1}{2} = 1.
\]

For \( n \geq 1 \), we have that

\[
\int_{0}^{\pi} \cos(n\theta) d\theta = 0,
\]

and so we need to show that

\[
\lim_{m \to \infty} \frac{1}{(q_m - 1)\sqrt{q_m^n}} \sum_{\chi \in \chi(q_m) \backslash \{\epsilon\}} (\alpha^n + \beta^n) = \begin{cases} 0, & n \text{ odd} \\ 1, & n \equiv 0 \pmod{4} \\ -1, & n \equiv 2 \pmod{4} \end{cases} \quad (3.2.7)
\]

where \( \alpha\chi \) and \( \beta\chi \) are obtained from Theorem 2.0.1. Here we may omit the trivial character \( \epsilon \) because its contribution to the summation is negligible in the limit as \( m \to \infty \). Fix some \( q = q_m \). We will consider first the non-square characters in \( \chi(q_m) \) and then the square characters. For non-square \( \chi \in \chi(q) \), we know that \( \alpha\chi + \beta\chi = 0 \) and that \( \alpha\chi\beta\chi = q \), which gives

\[
\{\alpha\chi, \beta\chi\} = \{i\sqrt{q}, -i\sqrt{q}\}.
\]

Then,

\[
\sum_{\chi \in \chi(q) \backslash \{\epsilon\}} (\alpha^n + \beta^n) = \sum_{\chi \in \chi(q) \backslash \{\epsilon\}} (i\sqrt{q})^n (1 + (-1)^n) = \frac{(q - 1)\sqrt{q^n}}{2} i^n (1 + (-1)^n).
\]

This gives that

\[
\lim_{m \to \infty} \frac{1}{(q_m - 1)\sqrt{q_m^n}} \sum_{\chi \in \chi(q_m) \backslash \{\epsilon\}} (\alpha^n + \beta^n) = \begin{cases} 0, & n \text{ odd} \\ 1, & n \equiv 0 \pmod{4} \\ -1, & n \equiv 2 \pmod{4} \end{cases} \quad (3.2.8)
\]

For square \( \chi \in \chi(q) \backslash \{\epsilon\} \), we can write \( \chi = \eta^2 \). Because \( \eta \neq \epsilon \) and \( \mu_q\eta \neq \epsilon \), we have by Proposition 3.1.2 that

\[
J(\eta, \mu_q) = \frac{G(\mu_q)G(\eta)}{G(\mu_q\eta)}, \quad J(\mu_q\eta, \mu_q) = \frac{G(\mu_q)G(\mu_q\eta)}{G(\eta)}.
\]

Furthermore, we have that

\[
(-\eta(-1) J(\eta, \mu_q)) \cdot (-\mu_q\eta(-1) J(\mu_q\eta, \mu_q)) = \mu_q(-1)G(\mu_q)^2 = q.
\]
Thus Proposition 3.2.1 implies that
\[ \{ \alpha, \beta \} = \{ -\eta (-1) J (\eta, \mu_q), -\mu_q \eta (-1) J (\mu_q \eta, \mu_q) \} . \]

Note that \( \eta \) and \( \mu_q \eta \) are exactly the two “square roots” of \( \chi \). We now obtain
\[ \sum_{\chi \in X (F_q^*) \setminus \{ \epsilon \}} (\alpha^n + \beta^n) = \sum_{\eta \in X (F_q) \setminus \{ \epsilon, \mu_q \}} (-1)^n (-J (\eta, \mu_q))^n . \]

Applying Proposition 3.2.2 for \( f (\phi) = \cos (n \phi) \), we obtain that
\[ \lim_{m \to \infty} \frac{1}{q_m - 1} \sqrt{q_m} \sum_{\chi \in X (F_{q_m}^*) \setminus \{ \epsilon \}} (\alpha^n + \beta^n) = 0 . \tag{3.2.9} \]

Summing (3.2.8) and (3.2.9) gives (3.2.7), which completes the proof. \( \square \)

### 3.3 The Case \( b \neq 0 \)

In this section we attempt to adapt the work of Adolphson in [8] to prove an equidistribution result for Legendre sums for the case \( b \neq 0, \pm 1 \).

If \( \chi \in X (F_q^*) \), then \( \chi^q = \chi \). Hence for all \( n \in \mathbb{Z}_{\geq 1} \) and all \( \chi \in X (F_q^*) \) we may define a “degree” of \( \chi \) by
\[ d_\chi := \min \left\{ k \in \mathbb{Z}_{\geq 1} : \chi^{q^k} = \chi \right\} \geq 1 , \]

Then, let
\[ X (F_q^*) := \bigcup_{n=1}^{\infty} \{ \chi \in X (F_q^*): d_\chi = n \} . \]

Note that for \( \chi \in X (F_q^*) \), the \( \alpha_\chi \) and \( \beta_\chi \) that we obtain from Theorem 2.0.1 (for any \( b \neq \pm 1 \)) satisfy \( |\alpha_\chi| = |\beta_\chi| = \sqrt{q^{d_\chi}} \). Define for \( n \in \mathbb{Z}_{\geq 1} \) the infinite product \( \mathcal{L}_{q,n} (T) \) by
\[ \mathcal{L}_{q,n} (T) = \prod_{\chi \in X (F_q^*) \setminus \{ \epsilon \}} \prod_{k=0}^{n} (1 - \alpha_\chi \beta_\chi^{n-k} T^{d_\chi})^{-1/d_\chi} . \tag{3.3.1} \]

**Conjecture 3.3.2.**

(a) The infinite product \( \mathcal{L}_{q,n} (T) \) is actually a polynomial in \( \mathbb{Z} [T] \).

(b) The degree of \( \mathcal{L}_{q,n} (T) \) is less than or equal to \( c_n \), where \( c_n \) is a constant independent of \( q \).

(c) If we write
\[ \mathcal{L}_{q,n} (T) = \prod_{i=1}^{c_n} (1 - \gamma_i T) , \tag{3.3.3} \]
then for all \( i \in \{ 1, 2, \ldots, c_n \} \), \( |\gamma_i| \leq \sqrt{q}^{n+1} \).
Theorem 3.3.4. Conjecture 3.3.2 implies Conjecture 0.0.2.

Proof. Just as in the proof of Proposition 3.2.2, it suffices to prove

$$\lim_{m \to \infty} \frac{1}{q_m - 1} \sum_{\chi \in X(\mathbb{F}_{q_m}^*)} f(\theta \chi) = \frac{2}{\pi} \int_0^\pi f(\theta) \sin^2(\theta) \, d\theta,$$

for $f(\theta) = \cos(n\theta)$, $n \in \mathbb{Z}_{\geq 0}$. The case $n = 0$ is straightforward:

$$\lim_{m \to \infty} \frac{1}{q_m} \sum_{\chi \in X(\mathbb{F}_{q_m}^*)} f(\theta \chi) = \lim_{m \to \infty} 1 = 1,$$

$$\frac{2}{\pi} \int_0^\pi \sin^2(\theta) \, d\theta = 1.$$

For $n \geq 1$, a simple computation shows that

$$\frac{2}{\pi} \int_0^\pi \cos(n\theta) \sin^2(\theta) \, d\theta = \begin{cases} -\frac{1}{2}, & n = 2, \\ 0, & n \neq 2. \end{cases}$$

For all $\chi \in X(\mathbb{F}_{q_m}^*) \setminus \{\epsilon\}$ we obtain from Theorem 2.0.1 numbers $\alpha_{\chi}, \beta_{\chi} \in \mathbb{C}$, and by (3.0.2),

$$\cos(n\theta) = \frac{1}{2} \left( \exp(i n\theta) + \exp(-i n\theta) \right) = \frac{(-1)^n}{2q_m^{n/2}} \left( \alpha_{\chi}^n + \beta_{\chi}^n \right).$$

Hence, we need to show that

$$\lim_{m \to \infty} \frac{1}{q_m - 1} \sqrt{q_m} \sum_{\chi \in X(\mathbb{F}_{q_m}^*) \setminus \{\epsilon\}} (\alpha_{\chi}^n + \beta_{\chi}^n) = \begin{cases} -1, & n = 2, \\ 0, & n \neq 2. \end{cases} \tag{3.3.5}$$

Fix some $q = q_m$. We will now apply Conjecture 3.3.2. Taking a logarithmic derivative of both sides of (3.3.1) gives

$$\frac{d}{dT} \mathcal{L}_{q,n}(T) = \sum_{\chi \in X(\mathbb{F}_{q}^*) \setminus \{\epsilon\}} \sum_{k=0}^n \left( -\frac{1}{\alpha_{\chi}^k} \frac{d}{dT} \log \left( 1 - \alpha_{\chi}^k \beta_{\chi}^{n-k} T^{d_{\chi}} \right) \right)$$

$$= \sum_{\chi \in X(\mathbb{F}_{q}^*) \setminus \{\epsilon\}} \sum_{k=0}^n \frac{\alpha_{\chi}^k \beta_{\chi}^{n-k} T^{d_{\chi}-1}}{1 - \alpha_{\chi}^k \beta_{\chi}^{n-k} T^{d_{\chi}}}. $$

Expanding in geometric series, this equals

$$\sum_{\chi \in X(\mathbb{F}_{q}^*) \setminus \{\epsilon\}} \sum_{k=0}^n \alpha_{\chi}^k \beta_{\chi}^{n-k} T^{d_{\chi}-1} \sum_{j=0}^{\infty} \left( \alpha_{\chi}^k \beta_{\chi}^{n-k} T^{d_{\chi}} \right)^j = \sum_{j=1}^{\infty} \sum_{\chi \in X(\mathbb{F}_{q}^*) \setminus \{\epsilon\}} \sum_{k=0}^n \left( \alpha_{\chi}^k \beta_{\chi}^{n-k} \right)^j T^{j \cdot d_{\chi}-1}. $$

24
Note that $jd_\chi - 1 = 0$ if and only if $j = 1$ and $\chi \in X(\mathbb{F}_q^*)$. Taking a logarithmic derivative of both sides of (3.3.3) and expanding in geometric series gives

$$\frac{d}{dT} L_{q,n}(T) = \sum_{i=1}^{c_n} \log (1 - \gamma_i T) = -\sum_{i=1}^{c_n} \gamma_i \sum_{j=0}^{\infty} (\gamma_i T)^j = -\sum_{j=0}^{\infty} \sum_{i=1}^{c_n} \gamma_i^{j+1} T^j.$$  

Comparing the constant terms on the right-hand sides of the previous two expressions gives for all $n \geq 1$ that

$$\sum_{\chi \in X(\mathbb{F}_q^*) \setminus \{\epsilon\}}^{n-1} \sum_{k=0}^{n} \alpha_\chi^k \beta_\chi^{n-k} = -\sum_{i=1}^{c_n} \gamma_i,$$

and so by Conjecture 3.3.2(c),

$$\left| \sum_{\chi \in X(\mathbb{F}_q^*) \setminus \{\epsilon\}}^{n-1} \sum_{k=0}^{n} \alpha_\chi^k \beta_\chi^{n-k} \right| \leq c_n \sqrt{q^{n+1}} \quad (3.3.6)$$

for all $n \geq 1$. This immediately implies (3.3.5) for $n = 1$. For $n \geq 2$, note that for $\chi \in X(\mathbb{F}_q^*) \setminus \{\epsilon\}$ we have because $\alpha_\chi \beta_\chi = q$ that

$$\sum_{k=0}^{n} \alpha_\chi^k \beta_\chi^{n-k} = \alpha_\chi^n + \beta_\chi^n + q \sum_{k=0}^{n-2} \alpha_\chi^k \beta_\chi^{n-k-2}. \quad (3.3.7)$$

For $n = 2$, summing the right-hand side of (3.3.7) over $\chi \in X(\mathbb{F}_q^*) \setminus \{\epsilon\}$ and using (3.3.6) gives

$$\left| \sum_{\chi \in X(\mathbb{F}_q^*) \setminus \{\epsilon\}} (\alpha_\chi^2 + \beta_\chi^2) + q (q - 1) \right| \leq c_n \sqrt{q^3},$$

which implies (3.3.5) for $n = 2$. Lastly, for $n \geq 3$, we use (3.3.6) and (3.3.7) to obtain

$$\left| \sum_{\chi \in X(\mathbb{F}_q^*) \setminus \{\epsilon\}} (\alpha_\chi^n + \beta_\chi^n) \right| \leq (c_n - c_{n-2}) \sqrt{q^{n+1}},$$

which gives (3.3.5) for $n \geq 3$. \hfill \blackqed

A Simulation Code

```python
#!/usr/bin/sage
from sage.all import *
from sage.plot.histogram import import Histogram
import numpy as np
```

25
```python
import matplotlib.pyplot as plt
import time
start_time = time.time()

q = 11**4
b = 2
# q = GF(q).multiplicative_generator()

angles = []
# converts Legendre sum to its corresponding angle, after
# correcting for rounding errors

def to_angle(s):
    s = CC(s).real()
    if abs(s) < 10**(-8):
        s = RR(0)
    elif abs(s) > 2 * sqrt(q):
        s = RR(2 * sqrt(q))
    return RR(arccos(s / (2 * sqrt(q))))

# generate array of mu_q(Q,b(x)) for all x
Mu = [1] * q

def mu(x):
    if x == 0:
        return 0
    if x.is_square():
        return 1
    return -1

for k in range(0, q-1):
    Mu[k+1] = mu((g**k)**2 + 2*b*(g**k) + 1)

# chi(g) where chi is the generator of X(F_q\ast) and g is the
# generator of F_q\ast

# array of chi(g) for all g in F_q\ast
N0 = np.array([0,1] + [gen_chi_g**j for j in range(1, q-1)])

angles.append(to_angle(np.dot(N0, Mu)))

# add angles corresponding to chi(g^i) for all g in F_q\ast and all i
# this corresponds to exponentiating every element of N0

for i in range(2, q):
    Ni = [x**i for x in N0]
    angles.append(to_angle(np.dot(Ni, Mu)))

print('Calculation took ' + str(time.time() - start_time) + ' s.

# phi(t)

t = np.arange(0.0, np.pi, 0.001)
s = (2 / np.pi) * np.sin(t)**2 #1 / (2*np.pi) + t * 0
plt.plot(t, s, lw=2)
plt.hist(angles, bins=200, normed=True)
plt.xlim(0, np.pi)
plt.ylim(0, 1.25)
```
References


