Alexander Krigsman

Equidistribution Theorems for Legendre Sums

Bachelor thesis

July 1, 2017

Thesis supervisor: Dr. Richard Griffon

Leiden University
Mathematical Institute

Contents

Introduction

Denote by q an odd prime power, and let $X\left(\mathbb{F}_q^*\right) := \mathrm{Hom}\left(\mathbb{F}_q^*, \mathbb{C}^*\right)$ be the group of multiplicative characters on the finite field $\mathbb{F}_q$ with q elements. We denote by $\mu_q \in X\left(\mathbb{F}_q^*\right)$ the quadratic character on $\mathbb{F}_q$, i.e. the unique character of order 2, and we denote by $\epsilon \in X\left(\mathbb{F}_q^*\right)$ 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 $\chi \in X\left(\mathbb{F}_q^*\right)$ 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 $b \in \mathbb{F}_q$, $\chi \in X\left(\mathbb{F}_q^*\right)$, 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 $\chi \in X\left(\mathbb{F}_q^*\right)$. This allows us to define a unique angle $\theta \in [0, \pi]$ associated to the pair (χ, b) by the equation

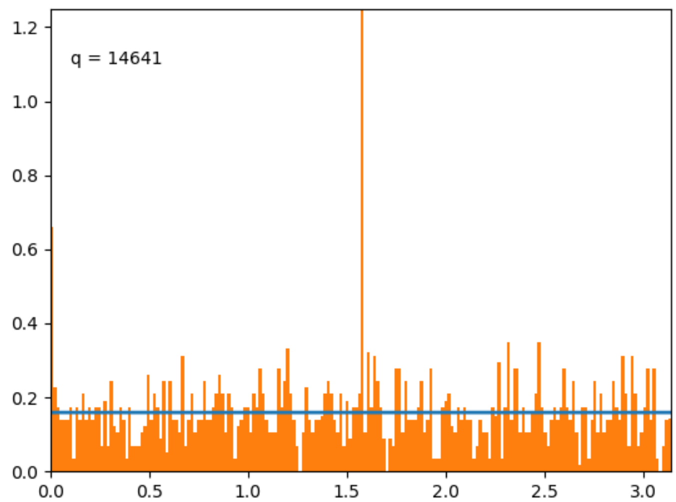
$$S_q(\chi; b) = 2\sqrt{q}\cos(\theta).$$

We attempt to study the distribution of these angles as $q \to \infty$ for fixed b and varying χ. 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 $\chi \in X\left(\mathbb{F}_{q_m}^*\right)$ let θ_χ be the angle associated to the Legendre sum $S_{q_m}(\chi; 0)$. Then the numbers $\{\theta_\chi\}_{\chi \in X\left(\mathbb{F}_{q_m}^*\right)}$ 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 $f : [0, \pi] \to \mathbb{R}$,*

$$\lim_{m\to\infty} \frac{1}{q_m - 1} \sum_{\chi \in X\left(\mathbb{F}_{q_m}^*\right)} f\left(\theta_\chi\right) = \frac{1}{2\pi} \int_0^\pi f\left(\theta\right) \mathrm{d}\theta + \frac{1}{2} f\left(\frac{\pi}{2}\right).$$

We motivate this theorem with the following graph. The angles corresponding to the Legendre sums $S_{11^4}\left(\chi; 0\right)$ for χ varying over all $\chi \in X\left(\mathbb{F}_{11^4}^*\right)$ were computed, and a histogram of them was plotted. Furthermore, overlaid on the graph is the constant line $\theta \mapsto 1/\left(2\pi\right)$.

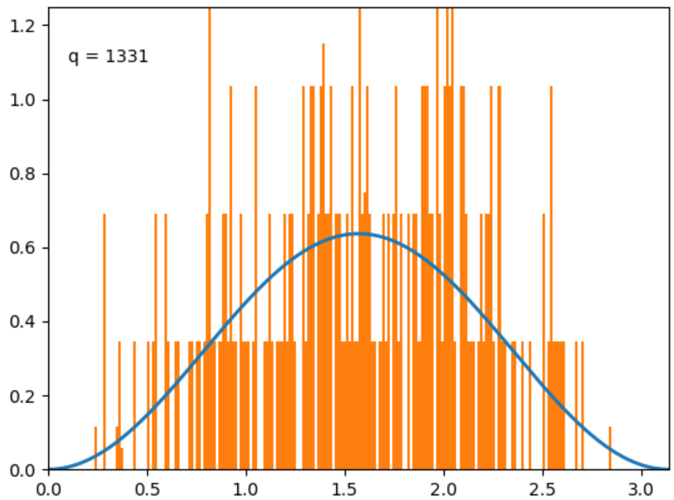


Furthermore, we reduce the following conjecture to the problem of proving that a particular infinite product converges to a polynomial.

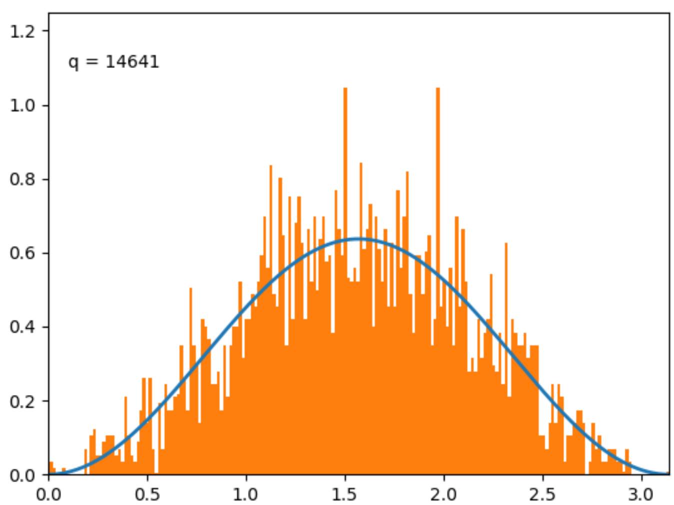
Conjecture 0.0.2. *Let $\{q_m\}_{m\geq 1}$ be a sequence of odd prime powers which tends to infinity. For all $m \geq 1$ take $b \in \mathbb{F}_{q_m} \setminus \{0, 1, -1\}$, and for all $\chi \in X\left(\mathbb{F}_{q_m}^*\right)$, let θ_χ be the angle associated to the Legendre sum $S_{q_m}\left(\chi;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

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

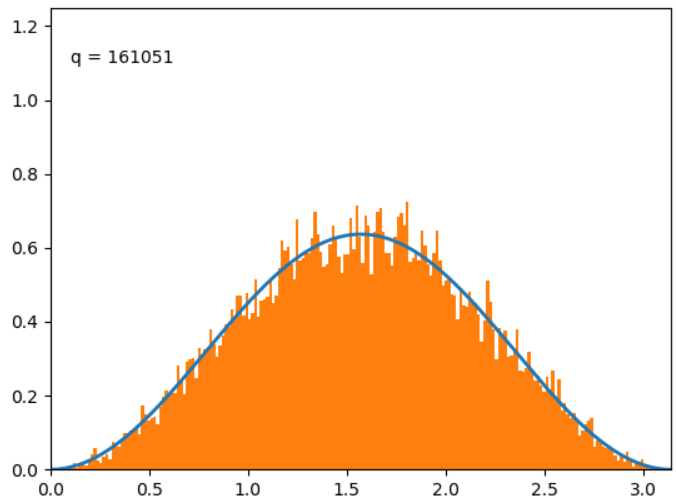
We motivate this conjecture with the following set of graphs. The angles corresponding to the Legendre sums $S_q\left(\chi; b\right)$ for $q = 11^3, 11^4, 11^5$, fixing $b = 2$ and varying χ over all $\chi \in X\left(\mathbb{F}_q^*\right)$, were computed, and histograms of them were plotted. Furthermore,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



Histogram of angles for $q = 11^3$



Histogram of angles for $q = 11^4$



Histogram of angles for $q = 11^5$

See Appendix A for the code used to produce these graphs.

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 $X\left(\mathbb{F}_q^*\right)$ 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

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

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

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

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

$$\#\left\{x \in \mathbb{F}_q : x^d = a\right\} = \sum_{\substack{\chi \in X\left(\mathbb{F}_q^*\right) \\ \chi^d = \epsilon}} \chi(a), \tag{1.1.3}$$

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

$$\#\left\{x \in \mathbb{F}_q : x^2 = a\right\} = 1 + \mu_q\left(a\right). \tag{1.1.4}$$

For proofs of these identities see for instance Chapter 8.1 of [1].

Proposition 1.1.5. *Consider $\chi \in X\left(\mathbb{F}_q^*\right)$. If χ is square, then $\chi\left(-1\right) = 1$, and if χ is non-square, then $\chi\left(-1\right) = -1$.*

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

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

Let n be a positive integer. Let $N_{\mathbb{F}_{q^n}/\mathbb{F}_q}$ be the norm of the field extension $\mathbb{F}_{q^n}/\mathbb{F}_q$, given by

$$N_{\mathbb{F}_{q^n}/\mathbb{F}_q}\left(\alpha\right) = \prod_{k=0}^{n-1} \alpha^{q^k}.$$

for $\alpha \in \mathbb{F}_{q^n}$. We recall the following properties of the norm.

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

$$\begin{aligned} N_{\mathbb{F}_{q^n}/\mathbb{F}_q}\left(\alpha\right) &\in \mathbb{F}_q, \\ N_{\mathbb{F}_{q^n}/\mathbb{F}_q}\left(\alpha\beta\right) &= N_{\mathbb{F}_{q^n}/\mathbb{F}_q}\left(\alpha\right) N_{\mathbb{F}_{q^n}/\mathbb{F}_q}\left(\beta\right), \\ N_{\mathbb{F}_{q^n}/\mathbb{F}_q}\left(\alpha x\right) &= x^n N_{\mathbb{F}_{q^n}/\mathbb{F}_q}\left(\alpha\right). \end{aligned}$$

Similarly, let $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}$ be the trace of the field extension $\mathbb{F}_{q^n}/\mathbb{F}_q$, given by

$$\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}\left(\alpha\right) = \sum_{k=0}^{n-1} \alpha^{q^k}.$$

We recall the following properties of the trace.

Proposition 1.1.7. *The trace $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}$ maps $\mathbb{F}_{q^n}$ onto $\mathbb{F}_q$. Furthermore, if we take $\alpha, \beta \in \mathbb{F}_{q^n}$ and $x \in \mathbb{F}_q$, then*

$$\begin{aligned} \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}\left(\alpha\right) &\in \mathbb{F}_q, \\ \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}\left(\alpha + \beta\right) &= \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}\left(\alpha\right) + \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}\left(\beta\right), \\ \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}\left(\alpha x\right) &= x \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}\left(\alpha\right). \end{aligned}$$

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

Let χ be a multiplicative character on $\mathbb{F}_q$. Proposition 1.1.6 allows us to lift χ to a character on $\mathbb{F}_{q^n}$ by composing with the norm: $\chi \circ N_{\mathbb{F}_{q^n}/\mathbb{F}_q} \in X\left(\mathbb{F}_{q^n}^*\right)$.

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*

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

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 φ 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 φ is an injective map between finite sets of the same cardinality, we have that φ 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 $x \in \mathbb{F}_q^*$,

$$\mu_q\left(Q_b\left(x^{-1}\right)\right) = \mu_q\left(\left(x^{-1}\right)^2 Q_b(x)\right) = \mu_q(Q_b(x)).$$

Using this fact, the complex conjugate of $S_q(\chi; b)$ is given by

$$\begin{aligned}\overline{S_q(\chi;b)} &= \chi(0)\,\mu_q(Q_b(0)) + \sum_{x\in\mathbb{F}_q^*} \overline{\chi(x)}\mu_q(Q_b(x)) \\ &= \chi(0)\,\mu_q(Q_b(0)) + \sum_{x\in\mathbb{F}_q^*} \chi\left(x^{-1}\right)\mu_q\left(Q_b\left(x^{-1}\right)\right) \\ &= S_q(\chi;b).\end{aligned}$$

(b)

$$\begin{aligned}S_q(\chi;\pm1) &= \sum_{x\in\mathbb{F}_q} \chi(x)\,\mu_q(Q_{\pm1}(x)) = \sum_{x\in\mathbb{F}_q} \chi(x)\,\mu_q(x\pm1)^2 \\ &= \sum_{x\in\mathbb{F}_q} \chi(x) = \begin{cases} q-1, & \chi=\epsilon \\ 0, & \chi\neq\epsilon \end{cases}.\end{aligned}$$

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

$$\begin{aligned}S_q(\epsilon;b) &= \sum_{x\in\mathbb{F}_q} \mu_q(Q_b(x)) = -q + \sum_{x\in\mathbb{F}_q} \left(1+\mu_q\left((x+b)^2-\Delta\right)\right) \\ &= -q + \sum_{x\in\mathbb{F}_q}\left(1+\mu_q\left(x^2-\Delta\right)\right) = -q + \sum_{x\in\mathbb{F}_q} \#\left\{y\in\mathbb{F}_q : y^2 = x^2-\Delta\right\} \\ &= -q + \#\left\{(x,y)\in\mathbb{F}_q^2 : (x+y)(x-y) = \Delta\right\} = -q+q-1 \\ &= -1.\end{aligned}$$

□

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 $\chi \in X\left(\mathbb{F}_q^*\right)$ and $b \in \mathbb{F}_q \setminus \{\pm1\}$. There exist $\alpha, \beta \in \mathbb{C}$ such that $\alpha\beta = q$ and such that for all $n \in \mathbb{Z}_{\geq 1}$,*

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

Here α and β implicitly depend on χ and b, and we will throughout this paper fix b and write α_χ, β_χ for the α, β corresponding to a particular character χ.

We also prove the following.

Theorem 2.0.2 (Riemann Hypothesis for Legendre Sums)**.** *The α and β 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 $\chi \in X\left(\mathbb{F}_q^*\right)$, 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 α^n and β^n to $S_{q^n}\left(\chi \circ N_{\mathbb{F}_{q^n}/\mathbb{F}_q}; b\right)$. After proving Theorem 2.0.1, we show that α and β have the desired magnitude.

2.1 Constructing α and β

Consider $b \in \mathbb{F}_q \setminus \{\pm 1\}$ and nontrivial $\chi \in X\left(\mathbb{F}_q^*\right)$. 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 $z_1 z_2 = 1$. Furthermore, because $b \neq \pm 1$, the discriminant $4\left(b^2 - 1\right)$ of Q_b is nonzero, and z_1 and z_2 are distinct. Denote by $\mathbb{F}_q^{\mathrm{m}}[T]$ the set of monic polynomials over $\mathbb{F}_q$. We define the map

$$\begin{aligned} \lambda : \mathbb{F}_q^{\mathrm{m}}[T] &\to \mathbb{C}, \\ f &\mapsto \chi\left((-1)^{\deg f} f(0)\right) \mu_q\left(f(z_1) f(z_2)\right), \end{aligned}$$

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

$$\begin{aligned} f(z_1) f(z_2) &= \sum_{1 \leq i,j \leq \deg f}^{\deg f} a_i a_j z_1^i z_2^j \\ &= \sum_{1 \leq i < j \leq \deg f} a_i a_j z_1^i z_2^j + \sum_{1 \leq i < j \leq \deg f} a_i a_j z_2^i z_1^j + \sum_{i=1}^{\deg f} a_i^2 (z_1 z_2)^i \\ &= \sum_{1 \leq i < j \leq \deg f} a_i a_j z_2^{j-i} + \sum_{1 \leq i < j \leq \deg f} a_i a_j z_1^{j-i} + \sum_{i=1}^{\deg f} a_i^2 \\ &= \sum_{1 \leq i < j \leq \deg f} a_i a_j (-2b) + \sum_{i=1}^{\deg f} a_i^2 \in \mathbb{F}_q. \end{aligned}$$

Furthermore, it is easy to see that λ 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*

$$\sigma(k) = \sum_{\substack{f \in \mathbb{F}_q^{\mathrm{m}}[T] \\ \deg f = k}} \lambda(f).$$

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

$$\begin{aligned}\sigma(2) &= \sum_{\substack{B\in\mathbb{F}_q[T]\\ \deg B<2}} \lambda(Q_b+B) = \sum_{x,y\in\mathbb{F}_q} \lambda(Q_b+xT+y)\\ &= \sum_{x,y\in\mathbb{F}_q} \chi(1+y)\,\mu_q((xz_1+y)(xz_2+y))\\ &= \sum_{x,y\in\mathbb{F}_q} \chi(1+y)\,\mu_q\left(x^2-2bxy+y^2\right)\\ &= \sum_{y\in\mathbb{F}_q} \chi(1+y) \sum_{x\in\mathbb{F}_q} \mu_q\left((x-by)^2-\Delta_y\right),\end{aligned}$$

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

$$\begin{aligned}\sum_{x\in\mathbb{F}_q} \mu_q\left((x-by)^2-\Delta_y\right) &= \sum_{a\in\mathbb{F}_q} \mu_q\left(a^2-\Delta_y\right)\\ &= -q + \sum_{a\in\mathbb{F}_q} \left(1+\mu_q\left(a^2-\Delta_y\right)\right)\\ &= -q + \sum_{a\in\mathbb{F}_q} \#\left\{z\in\mathbb{F}_q : z^2 = a^2-\Delta_y\right\}\\ &= -q + \#\left\{(a,z)\in\mathbb{F}_q^2 : \Delta_y = (a-z)(a+z)\right\}\\ &= -q + \#\left\{(u,v)\in\mathbb{F}_q^2 : \Delta_y = uv\right\}\\ &= \begin{cases} -1 & \Delta_y \neq 0,\\ q-1 & \Delta_y = 0\end{cases}.\end{aligned}$$

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,

$$\sigma(1) = \chi(1)(q-1) - \sum_{y\in\mathbb{F}_q^*} \chi(1+y) = q.$$

For polynomials f of degree $k \geq 3$, we consider the Euclidean division $f = AQ_b + B$ of f by Q_b, where A is monic of degree $k-2$ and $\deg B < 2$. As f varies over all monic polynomials of degree k, A varies over all monic polynomials of degree $k-2$, and b

varies over all polynomials of degree at most 2. Hence, we may write

$$\begin{aligned}
\sigma(k) &= \sum_{\substack{f\in\mathbb{F}_q^{\mathrm{m}}[T]\\ \deg f=k}} \lambda(f) = \sum_{\substack{A\in\mathbb{F}_q^{\mathrm{m}}[T]\\ \deg A=k-2}} \sum_{\substack{B\in\mathbb{F}_q[T]\\ \deg B<2}} \lambda(AQ_b+B)\\
&= \sum_{\substack{x_0,x_2,\dots,x_{k-3}\in\mathbb{F}_q\\ y_0,y_1}} \lambda\left(\left(T^{k-2}+\sum_{i=0}^{k-3} x_iT^i\right)Q_b+(y_1T+y_0)\right)\\
&= \sum_{\substack{x_0,x_2,\dots,x_{k-3}\in\mathbb{F}_q\\ y_0,y_1}} \chi\left((-1)^k(x_0+y_0)\right)\mu_q\left((y_1z_1+y_0)(y_1z_2+y_0)\right)\\
&= q^{k-1}\sum_{y_0,y_1\in\mathbb{F}_q} \mu_q\left((y_1z_1+y_0)(y_1z_2+y_0)\right)\sum_{x_0\in\mathbb{F}_q}\chi(x_0+y_0),
\end{aligned}$$

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

Now define the formal power series

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

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

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

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

2.2 Taking Powers of α and β

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

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

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

$$\begin{aligned}
L(z) &= \sum_{f\in\mathbb{F}_q^{\mathrm{m}}[T]} \lambda(f)\,z^{\deg f} = \prod_{\substack{f\in\mathbb{F}_q^{\mathrm{m}}[T]\\ \text{irreducible}}} \sum_{k=1}^{\infty}\lambda\left(f^k\right)z^{\deg f^k}\\
&= \prod_{\substack{f\in\mathbb{F}_q^{\mathrm{m}}[T]\\ \text{irreducible}}} \sum_{k=1}^{\infty}\lambda(f)^k\,z^{k\deg f} = \prod_{\substack{f\in\mathbb{F}_q^{\mathrm{m}}[T]\\ \text{irreducible}}} \frac{1}{1-\lambda(f)\,z^{\deg f}},
\end{aligned}$$

where in the last step we used the fact that the summation is a geometric series. □

Lemma 2.2.2. *For all $n \in \mathbb{Z}_{\geq 1}$,*

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

Proof. By (2.1.3) and Lemma 2.2.1,

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

Taking the logarithmic derivative of both sides and multiplying by $-z$ gives

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

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

$$\begin{aligned} - \sum_{\substack{f \in \mathbb{F}_q^{\mathrm{m}}[T] \\ \text{irreducible}}} \frac{\lambda(f)(\deg f) z^{\deg f}}{1 - \lambda(f) z^{\deg f}} &= - \sum_{\substack{f \in \mathbb{F}_q^{\mathrm{m}}[T] \\ \text{irreducible}}} \lambda(f)(\deg f) z^{\deg f} \sum_{k=0}^{\infty} \lambda(f)^k z^{k \deg f} \\ &= - \sum_{k=1}^{\infty} \sum_{\substack{f \in \mathbb{F}_q^{\mathrm{m}}[T] \\ \text{irreducible}}} \lambda(f)^k (\deg f) z^{k \deg f}. \end{aligned}$$

Substituting $n = k \deg f$, we obtain

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

We thus have that

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

Equating like coefficients gives the desired result. $\square$

Lemma 2.2.3. *Consider* $n \in \mathbb{Z}_{\geq 1}$ *and irreducible* $f \in \mathbb{F}_q^{\mathrm{m}}[T]$ *such that* $\deg f \mid n$. *Then for all roots* $\zeta \in \overline{\mathbb{F}_q}$ *of* f,

$$\lambda(f)^{n/\deg f} = \left(\chi \circ N_{\mathbb{F}_{q^n}/\mathbb{F}_q}\right)(\zeta)\, \mu_{q^n}\left(Q_b(\zeta)\right).$$

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

$$\lambda(f)^{n/\deg f} = \chi\left(\left(-1\right)^{\deg f} f(0)\right)^{n/\deg f} \mu_q\left(f(z_1)\, f(z_2)\right)^{n/\deg f}.$$

For the χ term,

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

For the μ_q term,

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

This gives the desired result. ☐

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

$$\begin{aligned}
-S_{q^n}\left(\chi \circ N_{\mathbb{F}_{q^n}/\mathbb{F}_q}; b\right) &= -\sum_{\zeta \in \mathbb{F}_{q^n}} \left(\chi \circ N_{\mathbb{F}_{q^n}/\mathbb{F}_q}\right)(\zeta)\, \mu_{q^n}\left(Q_b(\zeta)\right) \\
&= -\sum_{\substack{f \in \mathbb{F}_q^{\mathrm{m}}[T] \\ \text{irreducible} \\ \deg f \mid n}} \sum_{\substack{\zeta \in \overline{\mathbb{F}_q} \\ f(\zeta) = 0}} \left(\chi \circ N_{\mathbb{F}_{q^n}/\mathbb{F}_q}\right)(\zeta)\, \mu_{q^n}\left(Q_b(\zeta)\right) \\
&= -\sum_{\substack{f \in \mathbb{F}_q^{\mathrm{m}}[T] \\ \text{irreducible} \\ \deg f \mid n}} \lambda(f)^{n/\deg f} \deg f \\
&= \alpha^n + \beta^n.
\end{aligned}$$

2.3 The Magnitude of α and β

In order to show that $|\alpha| = |\beta| = \sqrt{q}$, we construct a smooth projective algebraic curve whose zeta function has among its roots α^{-1} and β^{-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 $\overline{\mathbb{F}_q}[X, Y]$, since $b \neq \pm 1$ implies that $Q_b\left(X^d\right)$ is not a square in $\overline{\mathbb{F}_q}[X]$. 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 $(x, y) = \left(\sqrt[d-1]{b}, 0\right)$, since d and q are coprime. Because $(0,0), \left(\sqrt[d-1]{b}, 0\right) \notin C_0$, 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

$$\begin{aligned}
\#C_0\left(\mathbb{F}_{q^n}\right) &= \#\left\{(x, y) \in \mathbb{F}_{q^n}^2 : y^2 = Q_b\left(x^d\right)\right\} = \sum_{x \in \mathbb{F}_{q^n}} \#\left\{y \in \mathbb{F}_{q^n} : y^2 = Q_b\left(x^d\right)\right\} \\
&= \sum_{x \in \mathbb{F}_{q^n}} \left(1 + \mu_{q^n}\left(Q_b\left(x^d\right)\right)\right) = q^n + \sum_{z \in \mathbb{F}_{q^n}} \#\left\{x \in \mathbb{F}_{q^n} : z = x^d\right\} \mu_{q^n}\left(Q_b(z)\right) \\
&= q^n + \sum_{z \in \mathbb{F}_{q^n}} \sum_{\substack{\chi \in X\left(\mathbb{F}_{q^n}^*\right) \\ \chi^d = \epsilon}} \chi(z)\, \mu_{q^n}\left(Q_b(z)\right) = q^n + \sum_{\substack{\chi \in X\left(\mathbb{F}_{q^n}^*\right) \\ \chi^d = \epsilon}} S_{q^n}(\chi; b).
\end{aligned}$$

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

$$\#C_0\left(\mathbb{F}_{q^n}\right) = q^n - 1 + \sum_{\substack{\chi \in X\left(\mathbb{F}_{q^n}^*\right) \\ \chi^d = \epsilon \\ \chi \neq \epsilon}} S_{q^n}(\chi; b).$$

By Lemma 1.1.8,

$$\sum_{\substack{\chi \in X\left(\mathbb{F}_{q^n}^*\right) \\ \chi^d = \epsilon \\ \chi \neq \epsilon}} S_{q^n}(\chi; b) = \sum_{\substack{\chi \in X\left(\mathbb{F}_{q}^*\right) \\ \chi^d = \epsilon \\ \chi \neq \epsilon}} S_{q^n}\left(\chi \circ N_{\mathbb{F}_{q^n}/\mathbb{F}_q}; b\right).$$

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

$$\#C_0\left(\mathbb{F}_{q^n}\right) = q^n - 1 - \sum_{\substack{\chi \in X\left(\mathbb{F}_{q}^*\right) \\ \chi^d = \epsilon \\ \chi \neq \epsilon}} \left(\alpha_\chi^n + \beta_\chi^n\right).$$

The projective closure $\widetilde{C_0}$ of C_0 is the set of solutions $[x:y:z] \in \mathbb{P}^2\left(\overline{\mathbb{F}_q}\right)$ to the polynomial equation $\tilde{f}\,(x,y,z) = 0$ where $\tilde{f}\,(x,y,z) = y^2 z^{2(d-1)} - x^{2d} - 2bx^d z^d - z^{2d}$. 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 $(\mu_1, \mu_2, \cdots, \mu_d, \mu_{d+1}) \in \mathbb{A}^{d+1}\left(\overline{\mathbb{F}_q}\right)$ satisfying

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

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 $(u,v) \mapsto \left(u, u^2, u^3, \ldots, u^d, v\right)$. Hence $\#C\left(\mathbb{F}_{q^n}\right) = \#C_0\left(\mathbb{F}_q^n\right)$ 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

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

The points at infinity are the points on $\widetilde{C} \cap \{\mu_0 = 0\}$. This gives two points at infinity, namely the points $[0 : \cdots : 0 : \pm 1 : 1]$, 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

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

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

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

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

We now calculate the zeta function for $\widetilde{C}$:

$$\begin{aligned} \log Z\left(\widetilde{C}/\mathbb{F}_q; T\right) &= \sum_{n=1}^{\infty} \frac{\#\widetilde{C}(\mathbb{F}_{q^n})}{n} T^n \\ &= \sum_{n=1}^{\infty} \frac{q^n+1}{n} T^n - \sum_{\substack{\chi \in X\left(\mathbb{F}_q^*\right) \\ \chi^d = \epsilon \\ \chi \neq \epsilon}} \sum_{n=1}^{\infty} \frac{\alpha_\chi^n + \beta_\chi^n}{n} T^n \\ &= \sum_{\substack{\chi \in X\left(\mathbb{F}_q^*\right) \\ \chi^d = \epsilon \\ \chi \neq \epsilon}} \log\left(\left(1-\alpha_\chi T\right)\left(1-\beta_\chi T\right)\right) - \log(1-T) - \log(1-qT), \end{aligned}$$

and so

$$Z\left(\widetilde{C}/\mathbb{F}_q; T\right) = \prod_{\substack{\chi \in X\left(\mathbb{F}_q^*\right) \\ \chi^d = \epsilon \\ \chi \neq \epsilon}} \left(1-\alpha_\chi T\right)\left(1-\beta_\chi T\right) \Big/ (1-T)(1-qT). \tag{2.3.1}$$

By the Riemann hypothesis for curves over finite fields, the inverses of the roots of $Z\left(\widetilde{C}/\mathbb{F}_q; T\right)$ 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 $b \in \mathbb{F}_q \setminus \{\pm 1\}$. By Theorem 2.0.1, for all nontrivial $\chi \in X\left(\mathbb{F}_q^*\right)$,

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

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

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

Equivalently,

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

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 $\psi(x) = \exp\left(\frac{2\pi i}{p}\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(x)\right)$. For multiplicative characters $\chi, \rho \in X\left(\mathbb{F}_q^*\right)$, denote by $G(\chi)$ and $J(\chi, \rho)$ the respective Gauss and Jacobi sums:

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

Recall the following properties of Gauss and Jacobi sums.

Proposition 3.1.1. *We have that*

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

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

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

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

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

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

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

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

Consider collections $(\chi_i)_{i=1}^m$ and $(\rho_i)_{j=1}^n$ 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

$$\begin{aligned}
&\mathrm{Hyp}_{m,n}\left(\psi, (\chi_i)_{i=1}^m, (\rho_j)_{i=1}^n\right)(\mathbb{F}_q, t) \\
&\qquad := \sum_{\substack{x_1,\ldots,x_m \in \mathbb{F}_q \\ y_1,\ldots,y_n \in \mathbb{F}_q \\ \prod_{i=1}^m x_i = t \prod_{j=1}^n y_j}} \psi\left(\sum_{i=1}^m x_i - \sum_{j=1}^n y_j\right)\left(\prod_{i=1}^m \chi_i(x_i)\right)\left(\prod_{j=1}^n \rho_j(y_j)\right).
\end{aligned}$$

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

$$\left|\mathrm{Hyp}_{m,n}\left(\psi, (\chi_i)_{i=1}^m, (\rho_j)_{i=1}^n\right)(\mathbb{F}_q, t)\right| \le R q^{w/2},$$

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

$$\left|\sum_{\substack{x_1,\ldots,x_n \in \mathbb{F}_q \\ \prod_{i=1}^n x_i = 1}} \psi\left(\sum_{i=1}^n x_i\right)\right| \le n q^{(n-1)/2}$$

(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*

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

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

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

so $S_q(\chi; 0) = 0$.

Suppose $\chi = \eta^2$ for some $\eta \in X\left(\mathbb{F}_q^*\right)$. Then, using (1.1.4), we have that

$$\begin{aligned} S_q(\chi;0) &= \sum_{x\in\mathbb{F}_q} \eta\left(x^2\right)\mu_q\left(x^2+1\right) = \sum_{y\in\mathbb{F}_q} \eta(y)\,\mu_q(y+1)\,\#\left\{x\in\mathbb{F}_q : x^2 = y\right\} \\ &= \sum_{y\in\mathbb{F}_q} \eta(y)\,\mu_q(y+1) + \sum_{y\in\mathbb{F}_q} \eta(y)\,\mu_q(y+1)\,\mu_q(y) \\ &= \sum_{y\in\mathbb{F}_q} \eta(-y)\,\mu_q(1-y) + \sum_{y\in\mathbb{F}_q} \mu_q\eta(-y)\,\mu_q(1-y) \\ &= \eta(-1)\,J\left(\overline{\eta},\mu_q\right) + \mu_q\eta(-1)\,J\left(\mu_q\overline{\eta},\mu_q\right), \end{aligned}$$

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

$$\lim_{m\to\infty} \frac{1}{q_m - 3} \sum_{\eta\in Y\left(\mathbb{F}_q^*\right)} f(\phi_\eta) = \frac{1}{2\pi}\int_0^{2\pi} f(\phi)\,\mathrm{d}\phi. \tag{3.2.3}$$

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

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

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

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

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

$$\begin{aligned} \overline{\sum_{\eta\in Y\left(\mathbb{F}_q^*\right)} (\eta(-1)\,J(\eta,\mu_q))^n} &= \sum_{\eta\in Y\left(\mathbb{F}_q^*\right)} \left(\mu_q\eta(-1)\sum_{x\in\mathbb{F}_q} \mu_q\eta(x)\,\mu_q(1-x)\right)^n \\ &= \sum_{\eta'\in Y\left(\mathbb{F}_q^*\right)} \left(\eta'(-1)\,J(\eta',\mu_q)\right)^n. \end{aligned}$$

Hence, we need to show that

$$\lim_{m\to\infty} \mathcal{M}_n\left(q_m\right) = 0$$

for all $n \geq 1$, where

$$\mathcal{M}_n\left(q\right) := \frac{1}{q-3} \sum_{\eta \in Y\left(\mathbb{F}_q^*\right)} \left(\frac{\eta\left(-1\right) J\left(\eta, \mu_q\right)}{\sqrt{q}}\right)^n$$

denotes the n-th normalized moment of the character sum given by $\eta\left(-1\right) J\left(\eta, \mu_q\right)$ for $\eta \in Y\left(\mathbb{F}_q^*\right)$ over the field $\mathbb{F}_q$. Fix some $q = q_m$. For $\eta \in Y\left(\mathbb{F}_q^*\right)$ we can write $J\left(\eta, \mu_q\right)$ as a product of Gauss sums by applying Proposition 3.1.2 as follows:

$$J\left(\eta, \mu_q\right) = \frac{1}{q} G\left(\eta\right) G\left(\mu_q\right) \overline{G\left(\eta\mu_q\right)} = \frac{\mu_q \eta\left(-1\right)}{q} G\left(\eta\right) G\left(\mu_q\right) G\left(\mu_q \overline{\eta}\right).$$

Then,

$$\mathcal{M}_n\left(q\right) = \frac{1}{q-3} \left(\frac{\mu_q\left(-1\right) G\left(\mu_q\right)}{\sqrt{q}}\right)^n \sum_{\eta \in Y\left(\mathbb{F}_q^*\right)} \left(\frac{G\left(\eta\right) G\left(\mu_q \overline{\eta}\right)}{q}\right)^n,$$

where $\mu_q\left(-1\right) G\left(\mu_q\right) / \sqrt{q}$ has magnitude 1. Because $G\left(\epsilon\right) = 0$, we have that

$$\begin{aligned} \sum_{\eta \in Y\left(\mathbb{F}_q^*\right)} \left(G\left(\eta\right) G\left(\mu_q \overline{\eta}\right)\right)^n &= \sum_{\eta \in X\left(\mathbb{F}_q^*\right)} \left(G\left(\eta\right) G\left(\mu_q \overline{\eta}\right)\right)^n - 2G\left(\epsilon\right)^n G\left(\mu_q\right)^n \\ &= \sum_{\eta \in X\left(\mathbb{F}_q^*\right)} \left(G\left(\eta\right) G\left(\mu_q \overline{\eta}\right)\right)^n, \end{aligned}$$

and so

$$\left|\mathcal{M}_n\left(q\right)\right| \leq \frac{1}{q-3} \left|\sum_{\eta \in X\left(\mathbb{F}_q^*\right)} \left(\frac{G\left(\eta\right) G\left(\mu_q \overline{\eta}\right)}{q}\right)^n\right|. \tag{3.2.4}$$

Expanding each Gauss sum gives

$$\begin{aligned} \sum_{\eta \in X\left(\mathbb{F}_q^*\right)} \left(G\left(\eta\right) G\left(\mu_q \overline{\eta}\right)\right)^n = \sum_{\eta \in X\left(\mathbb{F}_q^*\right)} &\left(\sum_{y_1, \ldots, y_n \in \mathbb{F}_q^*} \eta\left(\prod_{i=1}^n y_i\right) \psi\left(\sum_{i=1}^n y_i\right)\right) \\ &\cdot \left(\sum_{z_1, \ldots, z_n \in \mathbb{F}_q^*} \mu_q \overline{\eta}\left(\prod_{i=1}^n z_i\right) \psi\left(\sum_{i=1}^n z_i\right)\right). \end{aligned}$$

Exchanging sums, we see that this equals

$$\sum_{\substack{y_1, \ldots, y_n \\ z_1, \ldots, z_n \in \mathbb{F}_q^*}} \psi\left(\sum_{i=1}^n \left(y_i + z_i\right)\right) \mu_q\left(\prod_{i=1}^n z_i\right) \sum_{\eta \in X\left(\mathbb{F}_q^*\right)} \eta\left(\prod_{i=1}^n y_i \middle/ \prod_{i=1}^n z_i\right).$$

By (1.1.1), the rightmost term satisfies

$$\sum_{\eta \in X\left(\mathbb{F}_q^*\right)} \eta\left(\prod_{i=1}^n y_i \Big/ \prod_{i=1}^n z_i\right) = \begin{cases} q-1, & \prod_{i=1}^n y_i = \prod_{i=1}^n z_i \\ 0, & \text{otherwise} \end{cases}.$$

Hence,

$$\begin{aligned}\sum_{\eta \in X\left(\mathbb{F}_q^*\right)} & \left(G(\eta)\, G(\mu_q \overline{\eta})\right)^n \\ &= (q-1) \sum_{\substack{y_1,\dots,y_n \in \mathbb{F}_q \\ z_1,\dots,z_n \\ \prod_{i=1}^n y_i = \prod_{i=1}^n z_i}} \psi\left(\sum_{i=1}^n (y_i + z_i)\right) \mu_q\left(\prod_{i=1}^n z_i\right).\end{aligned}$$

Substituting $z_i \to -z_i$, this equals

$$(q-1)\, \mu_q\left((-1)^n\right) \sum_{\substack{y_1,\dots,y_n \in \mathbb{F}_q \\ z_1,\dots,z_n \\ \prod_{i=1}^n y_i = (-1)^n \prod_{i=1}^n z_i}} \psi\left(\sum_{i=1}^n (y_i - z_i)\right) \mu_q\left(\prod_{i=1}^n z_i\right).$$

Contained in this expression is the hypergeometric sum

$$\begin{aligned}\mathrm{Hyp}_{n,n} & \left(\psi, (\epsilon)_{i=1}^n, (\mu_q)_{i=1}^n\right)\left(\mathbb{F}_q, (-1)^n\right) \\ &= \sum_{\substack{y_1,\dots,y_n \in \mathbb{F}_q \\ z_1,\dots,z_n \\ \prod_{i=1}^n y_i = (-1)^n \prod_{i=1}^n z_i}} \psi\left(\sum_{i=1}^n (y_i - z_i)\right) \mu_q\left(\prod_{i=1}^n z_i\right).\end{aligned}$$

Combining Lemma 3.1.3 with (3.2.4), we get that

$$\left|\mathcal{M}_n(q)\right| \le \frac{n(q-1)}{\sqrt{q}\,(q-3)},$$

and so we can see that

$$\lim_{m\to\infty} \mathcal{M}_n(q_m) = 0.$$

□

Theorem 3.2.5 (Restatement of Theorem 0.0.1)**.** *Let $\{q_m\}_{m\ge 1}$ be a sequence of odd prime powers which tends to infinity. For a given m and all $\chi \in X\left(\mathbb{F}_{q_m}^*\right)$ let θ_χ be the angle associated to the Legendre sum $S_{q_m}(\chi; 0)$. Then the numbers $\{\theta_\chi\}_{\chi \in X\left(\mathbb{F}_{q_m}^*\right)}$ 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 $f : [0,\pi] \to \mathbb{R}$,*

$$\lim_{m\to\infty} \frac{1}{q_m - 1} \sum_{\chi \in X\left(\mathbb{F}_{q_m}^*\right)} f(\theta_\chi) = \frac{1}{2\pi}\int_0^\pi f(\theta)\,\mathrm{d}\theta + \frac{1}{2} f\left(\frac{\pi}{2}\right). \tag{3.2.6}$$

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:

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

$$\frac{1}{2\pi} \int_0^\pi \mathrm{d}\theta + \frac{1}{2} = 1.$$

For $n \geq 1$, we have that

$$\int_0^\pi \cos(n\theta)\,\mathrm{d}\theta = 0,$$

and so we need to show that

$$\lim_{m\to\infty} \frac{1}{(q_m - 1)\sqrt{q_m}^n} \sum_{\chi \in X\left(\mathbb{F}_{q_m}^*\right)\setminus\{\epsilon\}} \left(\alpha_\chi^n + \beta_\chi^n\right) = \begin{cases} 0, & n \text{ odd} \\ 1, & n \equiv 0 \pmod 4 \\ -1, & n \equiv 2 \pmod 4 \end{cases}, \tag{3.2.7}$$

where α_χ and β_χ are obtained from Theorem 2.0.1. Here we may omit the trivial character ϵ 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 $X\left(\mathbb{F}_q^*\right)$ and then the square characters. For non-square $\chi \in X\left(\mathbb{F}_q^*\right)$, 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,

$$\sum_{\substack{\chi \in X\left(\mathbb{F}_q^*\right) \\ \chi \text{ non-square}}} \left(\alpha_\chi^n + \beta_\chi^n\right) = \sum_{\substack{\chi \in X\left(\mathbb{F}_q^*\right) \\ \chi \text{ non-square}}} (i\sqrt{q})^n \left(1 + (-1)^n\right) = \frac{(q-1)\sqrt{q}^n}{2} i^n \left(1 + (-1)^n\right).$$

This gives that

$$\lim_{m\to\infty} \frac{1}{(q_m - 1)\sqrt{q_m}^n} \sum_{\substack{\chi \in X\left(\mathbb{F}_{q_m}^*\right) \\ \chi \text{ non-square}}} \left(\alpha_\chi^n + \beta_\chi^n\right) = \begin{cases} 0, & n \text{ odd} \\ 1, & n \equiv 0 \pmod 4 \\ -1, & n \equiv 2 \pmod 4 \end{cases}. \tag{3.2.8}$$

For square $\chi \in X\left(\mathbb{F}_q^*\right) \setminus \{\epsilon\}$, we can write $\chi = \eta^2$. Because $\eta \neq \epsilon$ and $\mu_q\eta \neq \epsilon$, we have by Proposition 3.1.2 that

$$J(\overline{\eta}, \mu_q) = \frac{G(\mu_q)\,G(\overline{\eta})}{G(\mu_q\overline{\eta})}, \qquad J(\mu_q\overline{\eta}, \mu_q) = \frac{G(\mu_q)\,G(\mu_q\overline{\eta})}{G(\overline{\eta})}.$$

Furthermore, we have that

$$(-\eta(-1)\,J(\overline{\eta}, \mu_q)) \cdot (-\mu_q\eta(-1)\,J(\mu_q\overline{\eta}, \mu_q)) = \mu_q(-1)\,G(\mu_q)^2 = q.$$

Thus Proposition 3.2.1 implies that

$$\{\alpha_\chi, \beta_\chi\} = \{-\eta(-1) J(\overline{\eta}, \mu_q), -\mu_q \eta(-1) J(\mu_q \overline{\eta}, \mu_q)\}.$$

Note that η and $\mu_q \eta$ are exactly the two "square roots" of χ. We now obtain

$$\sum_{\substack{\chi \in X(\mathbb{F}_q^*) \setminus \{\epsilon\} \\ \chi \text{ square}}} \left(\alpha_\chi^n + \beta_\chi^n\right) = \sum_{\eta \in X(\mathbb{F}_q^*) \setminus \{\epsilon, \mu_q\}} \eta(-1)^n \left(-J(\overline{\eta}, \mu_q)\right)^n.$$

Applying Proposition 3.2.2 for $f(\phi) = \cos(n\phi)$, we obtain that

$$\lim_{m \to \infty} \frac{1}{(q_m - 1)\sqrt{q_m}^n} \sum_{\substack{\chi \in X(\mathbb{F}_{q_m}^*) \setminus \{\epsilon\} \\ \chi \text{ square}}} \left(\alpha_\chi^n + \beta_\chi^n\right) = 0. \tag{3.2.9}$$

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

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 $\chi \in X(\mathbb{F}_q^*)$, then $\chi^q = \chi$. Hence for all $n \in \mathbb{Z}_{\geq 1}$ and all $\chi \in X(\mathbb{F}_{q^n}^*)$ we may define a "degree" of χ by

$$d_\chi := \min\left\{k \in \mathbb{Z}_{\geq 1} : \chi^{q^k} = \chi\right\} \geq 1,$$

Then, let

$$X\left(\overline{\mathbb{F}_q}^*\right) := \bigsqcup_{n=1}^{\infty} \left\{\chi \in X(\mathbb{F}_{q^n}^*) : d_\chi = n\right\}.$$

Note that for $\chi \in X\left(\overline{\mathbb{F}_q}^*\right)$, the α_χ and β_χ 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

$$\mathcal{L}_{q,n}(T) = \prod_{\chi \in X\left(\overline{\mathbb{F}_q}^*\right) \setminus \{\epsilon\}} \prod_{k=0}^{n} \left(1 - \alpha_\chi^k \beta_\chi^{n-k} T^{d_\chi}\right)^{-1/d_\chi}. \tag{3.3.1}$$

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

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

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

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

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

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

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

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

$$\cos\left(n\theta_\chi\right) = \frac{1}{2}\left(\exp\left(in\theta_\chi\right) + \exp\left(-in\theta_\chi\right)\right) = \frac{\left(-1\right)^n}{2\sqrt{q_m}^n}\left(\alpha_\chi^n + \beta_\chi^n\right).$$

Hence, we need to show that

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

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

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

Expanding in geometric series, this equals

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

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

$$\frac{\mathrm{d}}{\mathrm{d}T}\mathcal{L}_{q,n}\left(T\right) = \sum_{i=1}^{c_n} \frac{\mathrm{d}}{\mathrm{d}T} \log\left(1 - \gamma_i T\right) = -\sum_{i=1}^{c_n} \gamma_i \sum_{j=0}^{\infty} \left(\gamma_i T\right)^j = -\sum_{j=0}^{\infty}\sum_{i=1}^{c_n} \gamma_i^{j+1} T^j.$$

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

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

and so by Conjecture 3.3.2(c),

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

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

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

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

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

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

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

which gives (3.3.5) for $n \geq 3$. □

A Simulation Code

```
#!/usr/bin/sage

from sage.all import *
from sage.plot.histogram import Histogram
import numpy as np
```

```
import matplotlib.pyplot as plt

import time
start_time = time.time()

q = 11**4
b = 2 #0
g = 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
gen_chi_g = CC(exp(2*pi*I / (q-1)))

# 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.')

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)
```

```
plt.text(0.1, 1.1, "q = " + str(q))
plt.show()
```

References

[1] Kenneth Ireland and Michael Rosen. *A Classical Introduction to Modern Number Theory*. Springer-Verlag, 1990.

[2] Serge Lang. *Algebra*. Springer-Verlag, revised third edition, 2002.

[3] Harald Niederreiter and Chaoping Xing. *Algebraic Geometry in Coding Theory and Cryptography*. Princeton University Press, 2009.

[4] Nicholas Katz. *Exponential Sums and Differential Equations*. Princeton University Press, 1990.

[5] Pierre Deligne. La conjecture de Weil : II. *Publications Mathématiques de l'IHÉS*, 52:137–252, 1980.

[6] Emmanuel Kowalski. A survey of algebraic exponential sums and some applications. 2011.

[7] Walter Rudin. *Principles of Mathematical Analysis*. McGraw-Hill Book Co., New York, third edition, 1976. International Series in Pure and Applied Mathematics.

[8] Alan Adolphson. On the distribution of angles of Kloosterman sums. *Journal für die reine und angewandte Mathematik*, 395:214–220, 1989.