The Zeros of Dirichlet Series of Cubic Gauss Sum over Function Fields

Nikol Metry

A Thesis
In the Department of
Mathematics and Statistics

Presented in Partial Fulfillment of the Requirements
For the Degree of
Master of Science (Mathematics and Statistics)

at Concordia University
Montreal, Quebec, Canada

August 2025

CONCORDIA UNIVERSITY
School of Graduate Studies

This is to certify that the thesis prepared

By: Metry, Nikol

Entitled: The Zeros of Dirichlet Series of Cubic Gauss Sums over Function Fields

and submitted in partial fulfillment of the requirements for the degree of

Master of Science

complies with the regulations of the University and meets the accepted standards with respect to originality and quality.

Signed by the final examining committee:

____________________ Chair
Dr. Giovanni Rosso

____________________ Examiner
Dr. Carlo Pagano

____________________ Examiner

____________________ Thesis Supervisor(s)
Dr. Chantal David

____________________ Thesis Supervisor(s)

Approved by ____________________
Dr. Lea Popovic Chair of Department or Graduate Program Director

____
Dr. Pascale Sicotte Dean of Faculty of Arts & Science

Abstract

The Zeros of Dirichlet Series of Cubic Gauss Sums over Function Fields

Nikol Metry

Since the Gauss sums are not multiplicative, the Dirichlet series of nth order Gauss sums do not have an Euler product. Therefore, they are not expected to satisfy the Riemann Hypothesis. Over $\mathbb{F}_q(t)$, the Dirichlet series of cubic Gauss sums are polynomials in $u = q^{-s}$, which reduces the task of finding the zeros of the series to computing the roots of a polynomial. In this work, we will discuss the challenges that arise when computing these roots and present numerical data on them.

Contents

1 Introduction **1**

2 Properties of function fields **4**

3 Characters of order d over $\mathbb{F}_q[x]$ **9**

4 Gauss sums **12**

5 The Dirichlet series of Gauss sums **16**

6 Algorithm and Computations **23**

6.1 Multiplicative character. 23

6.2 Additive character. 23

6.3 Gauss sum. 24

6.4 Residue. 25

6.5 Technical. 26

7 Results **26**

8 Graphs **29**

8.1 Linear 29

8.2 Quadratic 35

9 References **39**

1 Introduction

Gauss sums are fundamental objects in number theory. If we let χ denote a primitive Dirichlet character on $\mathbb{Z}/p\mathbb{Z}$ and let $\xi = e^{2\pi i/p}$ be a primitive p-th root of unity, the Gauss sum of χ is given by

$$g(\chi) = \sum_{t=1}^{p-1} \chi(t)\xi^{t/p}.$$

If $\chi(a) = \left(\frac{a}{p}\right)$ is a Legendre symbol, then the exact value of the corresponding quadratic Gauss sum was found by Gauss himself and is given by

$$g(\chi) = \begin{cases} \sqrt{p} & \textit{if } p \equiv 1 \mod 4, \\ i\sqrt{p} & \textit{if } p \equiv 3 \mod 4. \end{cases} \tag{1}$$

However, Gauss sums of higher order behave very differently.

We will be particularly interested in cubic Gauss sums. We let π be a prime in $\mathbb{Z}[\omega]$, where $\omega = \frac{-1+\sqrt{-3}}{2}$, such that $N\pi = p \equiv 1 \mod 3$, and let χ_π be a cubic residue character modulo π. In such a setting, we are able to define a Gauss up to a cube root.

Proposition 1.1 (Lemma 9.4.1, [IR90])**.**

$$g(\chi_\pi)^3 = p\pi.$$

But the exact cube root is not as easy to find. Trying to find a relation between the cube root of unity and the conductor of the Gauss sum, Kummer considered the frequency of $S_p = \Re(2g(\chi_p))$ falling into the intervals

$$I_1 = [\sqrt{p}, 2\sqrt{p}],\ I_2 = (-\sqrt{p}, \sqrt{p}),\ I_3 = [-2\sqrt{p}, \sqrt{p}],$$

for primes up to 500. Surprisingly, the ratio he observed was approximately $3 : 2 : 1$, although the values were expected to be equidistributed.

The work on the problem continued in the 20th century with the rise of computers, which allowed to extend the computations beyond those of Kummer. Further work did not shed much light on how to determine the cube root of unity, but it did cast doubt on Kummer's conclusions. In 1953, J. von Neumann and H.H. Goldstein considered all the primes up to 9973 and obtained the ratio $4 : 3 : 2$, which still did not fit the equidistribution criteria but was a step towards it. Subsequent computations further reinforced the idea that cubic Gauss sums were equidistributed, but it was not until 1979 that this was proved by Heath-Brown and Patterson in [PHB79], using the seminal work of Kubota on the theory of metaplectic forms ([Kub69], [Kub06]) and earlier work of Patterson ([Pat78]).

One of the reasons which makes the distribution of Gauss sums so mysterious is that they are not multiplicative. For $(\pi_1, \pi_2) = 1$, we have

$$g(\chi_{\pi_1\pi_2}) = \left(\frac{\pi_1}{\pi_2}\right)_3 g(\chi_{\pi_2})g(\chi_{\pi_1}).$$

Using the theory of metaplectic forms, it can be proven that the Dirichlet series of cubic Gauss sums satisfies a functional equation ralating s to $s-2$ and a meromorphic continuation to $\mathbb{C}$ with possible simple poles at $s = \frac{2}{3}$ and $\frac{4}{3}$.

In this thesis, we study the Dirichlet series of cubic shifted Gauss sums over function field $\mathbb{F}_q[x]$ for $q \equiv 1 \mod 6$, which are defined similarly as their number field counterparts :

$$G(V, f) = \sum_{a \mod f} \left(\frac{a}{f}\right)_3 e\left(\frac{aV}{f}\right).$$

We will define in details the cubic residue symbol $\left(\frac{\cdot}{\cdot}\right)_3$ in Chapter 3 and the exponential $e(\cdot)$ in the beginning of Chapter 4. The main objective of this work is to study the distribution of the zeros of the Dirichlet series of cubic Gauss sum. For $0 \leq i \leq 2$ and $u = q^{-s}$, we define

$$\psi(V, i, u) = (1 - u^3 q^3)^{-1} \sum_{\substack{F \in \mathcal{M}_q \\ \deg F \equiv i \mod 3}} G(V, F) u^{\deg f}.$$

As in the number field setting, the Gauss sums over function fields are not multiplicative, and this series does not have an Euler product. Therefore, despite having an analytic continuation and a functional equation, we do not expect it to vanish solely on the critical line.

As we will see in Section 5,

$$\psi(V, i, u) = \frac{u^i P(V, i, u^3)}{1 - q^4 u^3}, \tag{2}$$

where $P(V, i, u^3)$ is a polynomial of degree at most $\left[\frac{1+\deg V - i}{3}\right]$ in u^3. This reduces the search for zeros to solving the polynomial $P(V, i, u^3)$. Rearranging the terms in (1), we obtain

$$P(V, i, u^3) = u^{-i} \psi(V, i, u)(1 - q^4 u^3) \tag{3}$$

Further expanding (3), we can see that the coefficients of the polynomial are mainly the combinations of

$$C(V, m) = \sum_{f \in \mathcal{M}_{q,m}} G(V, f)$$

for $V \in \mathbb{F}_q[x]$, $m \in \mathbb{Z}^+$. There are q^m monic polynomials of degree m, and when computing one such object for a single V, we are iterating over all of them. Moreover, if $\deg V = m$, then the total number of summations in a Gauss sum, by definition, is q^m. Thus, we must perform q^{2m} additions in total, not taking into account the complexity of computing each summand in a Gauss sum, that is $\left(\frac{a}{f}\right)_3 e\left(\frac{aV}{f}\right)$.

As seen in the equation (2), $\psi(V, i, u)$ has a simple pole at the point $u = q^{-4/3}$. Let $\rho(V, i)$ denote the residue of $\psi(V, i, u)$ at $u^3 = q^{-4}$. As we will see in Section 5,

$$\rho(V, i) = P(V, i, q^{-4}).$$

David, Florea and Lalin in [DFL22] have given a formula for $\rho(V, i)$ that does not require a computation of the coefficients of $P(V, i, u^3)$, providing conditions for the vanishing of the residue $\rho(V, i)$, and therefore for $P(V, i, u^3)$ at $u^3 = q^{-4}$. Thus, we will refer to $q^{-4/3}$ as a trivial zero of $P(V, i, u^3)$ and will not consider $V \in \mathbb{F}_q[t]$, for which $P(V, 0, q^{-4/3}) = 0$.

In summary, to compile a comprehensive dataset of zeros of $P(V, i, u^3)$ we want to compute their roots for all appropriate inputs V, i.e. all monic square-free polynomials.

The maximum possible value of m in $C(V, m)$, appearing in a polynomial $P(V, i, x)$ of fixed degree n, is $i + 3n$, which brings the number of operations to $O(q^{3n})$.

Therefore, we have an exponential growth both in the size of the coefficients and in the number of inputs. Whereas the roots of the polynomial can be found using any root-finding algorithm, the real difficulty lies in computing the polynomial itself, particularly its coefficients. Thus, most of the work is centered on optimizing the computational process.

As we cannot avoid the exponential growth at the number of inputs, we will focus on minimizing the complexity of a single computation. There are two observations that would lead to a facilitated computational process.

First, notice that if pick an irreducible $a \in \mathbb{F}_q[t]$ of degree n, then we can associate $\mathbb{F}_q[t]/(a)$ with $\mathbb{F}_{q^n}[t]$, which would enable one to apply the Hasse-Davenport theorem to a Gauss sum modulo a. In [Pat07], Patterson elaborated on this observation, leading to the following theorem.

Theorem 1.2. *Let $V, f \in \mathbb{F}_q[x]$ be coprime. Then we have*

$$G(V, f) = \mu(V)\left(\frac{-f}{V}\right)_3^{-1}\left(\frac{f'}{f}\right)(-\tau(\chi_3))^{\deg f}$$

where f' denotes the derivative of f with respect to t.

The theorem allows us to avoid a lengthy summation. However, it is not the panacea as it still has limitations and requires the shift V and a conductor f to be coprime.

Next, observe that a Gauss sum is basically a discrete Fourier transform. Thus, if we treat polynomials as vectors with entries being their coefficients, and if we choose a correct linear functional to use within the exponential function, then we can apply the Fast Fourier Transform algorithm. This is the tool that we will be making use of in the case when the shift and the conductor are not coprime. Obviously, it will be more computationally demanding than the formula given above, but it is compensated for by the fact that, for a fixed $V \in \mathbb{F}_q[t]$, the majority of polynomials will be coprime to it.

In Section 2, we establish the required theory of function fields, which we will later need in Section 4 to prove one of the crucial theorems of the thesis. In Section 3, we will define the multiplicative character of order d over $\mathbb{F}_q[x]$ and elaborate on its properties. In section 4, we apply the theory from Section 1 to define the additive character on $\mathbb{F}_q[x]$ and then talk in more detail about Gauss sums. Section 5 focuses the Dirichlet series of cubic Gauss sums. In Section 6, we describe the algorithm used to compute the zeros of the Dirichlet series and discuss drawbacks, advantages and limitations of the methods used.

In Section 7, we present and discuss the data we obtained. To date, we have calculated the roots of more than 100,000 polynomials $P(V, i, u^3)$, covering all the linear cases and some quadratic ones. It has been sufficient to make some conjectures about the size and accumulation points of the roots. In Section 8, the graphs are presented.

2 Properties of function fields

The material of this section is based on the chapters 1.1, 1.2, 4.1 and 4.2 of [Sti09].

Definition 2.1. *An algebraic function field F/K of one variable over K is an extension field F containing K such that F is a finite extension of $K(x)$, where $x \in F$ is transcedental over K.*

The simplest example of a function field would be a rational function field, that is when $F = K(x)$ for some $x \in F$ transcendental over K.

Definition 2.2. *A valuation ring of the function field F/K is a ring $\mathcal{O} \subseteq F$ with following properties:*

1. $K \subsetneqq \mathcal{O} \subsetneqq F$
2. *For every $t \in F$, either $t \in \mathcal{O}$ or $t^{-1} \in \mathcal{O}$*

In the case of a rational function field $K(x)$, we can pick an irreducible monic polynomial $p(x) \in F$ and consider the set

$$\mathcal{O}_{p(x)} = \left\{ \frac{g(x)}{h(x)} \middle| g(x), h(x) \in K[x],\ p(x) \nmid h(x) \right\}$$

This set is a valuation ring. Furthermore, for two distinct monic irreducible polynomials $q(x), p(x)$, their corresponding valuation rings are also distinct. A valuation ring $\mathcal{O}$ has a unique maximal ideal $P = \mathcal{O}/\mathcal{O}^\times$. Indeed, if $x \in P,\ z \in \mathcal{O}$, then xz cannot be a unit and therefore is in P. Then, for $x, y \in P$, we can assume that $xy^{-1} \in \mathcal{O}$ (since, by definition of the valuation ring, we have $xy^{-1} \in \mathcal{O}$ or $x^{-1}y \in \mathcal{O}$) and then $x + y = y(1 + xy^{-1}) \in P$, so that P is an ideal. The maximality of P follows from the fact that no ideal can contain a unit and therefore, by definition of P, it is the biggest non-trivial ideal.

Definition 2.3. 1. *A place P of a function field F is the maximal ideal of some valuation ring $\mathcal{O}$. Every element $t \in P$ such that $P = t\mathcal{O}$ is called a prime element for P.*

2. *For each place P, we associate a discrete valuation v_P as follows: choose a prime element t for P. Then every non-zero element $z \in P$ can be written as $z = t^n a$, where $a \in \mathcal{O}^\times$ and $n \in \mathbb{Z},\ n \geq 1$. Define $v_P(z) := n$ and $v_P(0) := \infty$.*

Every valuation ring $\mathcal{O}$ is uniquely defined by its maximal ideal P, that is, $\mathcal{O} = \{z \in F \mid z \notin P\}$. Hence, $\mathcal{O}_P := \mathcal{O}$ is called *the valuation ring of the place P*. We let $F_P := \mathcal{O}_P/P$ be the residue class field of P. Then the $\deg P = [F_P : K]$ is called the *degree of P*.

We are particularly interested in the following valuation ring and place of $F/K(x)$:

$$\mathcal{O}_\infty = \{\frac{f(x)}{g(x)} \mid f(x), g(x) \in K[x],\ \deg f(x) \leq \deg g(x)\}$$

with maximal ideal

$$P_\infty = \{\frac{f(x)}{g(x)} \mid f(x), g(x) \in K(x),\ \deg f(x) < \deg g(x)\}.$$

The place is called the *infinite place.*

Proposition 2.4. *Let $P = P_\infty$ be the infinite place defined as above. Then* $\deg P_\infty = 1$*. A prime element of P_∞ is $1/x$. The corresponding discrete valuation is given by*

$$v_\infty(f(x)/g(x)) = \deg g(x) - \deg f(x)$$

where $f(t), g(t) \in K[x]$

Proof. First, we prove that $\deg P_\infty = 1$. Consider a map $\varphi : \mathcal{O}_\infty \to K$ given by $z \mapsto \frac{a_n}{b_m}$, where $z = \frac{a_n x^n + \ldots + a_0}{b_m x^m + \ldots + b_0}$. It is a ring homomorphism with the kernel being P_∞. Furthermore, it is surjective: let $a \in K$, then $z = \frac{ax^n + \ldots + a_0}{x^m + \ldots + b_0}$ is sent to a. Therefore, $F_P = \mathcal{O}_\infty / P \simeq K$.

Now, we show the prime element. Consider $z = f(x)/g(x) \in P$, so that $\deg f < \deg g$. Then

$$z = \frac{1}{x} \cdot \frac{xf}{g}.$$

Since $1/x \in P$ and $\deg xf \leq \deg g$, then $z \in (1/x)\mathcal{O}_\infty$. The reverse inclusion is trivial. It follows that P is generated by $1/x$. □

From now on, we assume K to be perfect and the full constant field of F.

Definition 2.5. *Let P be a place of F/K. The completion of F with respect to the valuation v_P is called the P-adic completion of F. We denote this completion by $\hat{F}_P$ and the valuation of $\hat{F}_P$ by v_P.*

Theorem 2.6. *Let P be a place of degree one with a prime element $t \in F$ and let $\hat{F}_P$ be its completion with respect to v_P. Then for every $z \in \hat{F}_P$ has a unique representation of the form*

$$z = \sum_{i=n}^{\infty} a_i t^i$$

with $n \in \mathbb{Z}$ and $a_i \in K$. This representation is called P-adic power series expansion of z with respect to t. Conversely, if $(c_i)_{i \geq n}$ is a sequence in K, then the series $\sum_{i=n}^{\infty} c_i t^i$ converges in $\hat{F}_P$, and we have

$$v_P(\sum_{i=n}^{\infty} c_i t^i) = \min\{i \mid c_i \neq 0\}$$

Proof. To prove the existence of the representation consider $z \in \hat{F}_P$, we choose an integer $n \leq v_P(z)$. Since F is dense in $\hat{F}_P$, there exists $y \in F$ such that $v_P(z - y) > n$. By the triangle inequality, we have $v_P(y) > n$ and $v_P(yt^{-n}) > 0$. Since P is a place of degree one, then $F_P \simeq K$, and therefore there is an element $a_n \in K$ such that, essentially, $yt^{-n} \equiv a_n \mod P$. This implies that $v_P(yt^{-n} - a_n) > 0$ and $v_P(y - t^n a_n) > n$. Then

$$v_P(z - a_n t^n) = v_P((z - y) + (yt^{-n} - a_n)) > n.$$

Similarly, we can obtain a_{n+1} with

$$v_P(z - a_n t^n - a_{n+1} t^{n+1}) > n + 1.$$

Continuing with this construction, we can build a sequence $(a_i)_{i=n}^{\infty}$ in K such that

$$v_P(z - \sum_{i=n}^{m} a_i t^i) > m,$$

where $m > n$. This is exactly the definition of the limit in the valued space, that is,

$$z = \sum_{i=n}^{\infty} a_t^i.$$

To prove uniqueness, assume that z has another representation, namely

$$z = \sum_{i=n}^{\infty} a_i t^i = \sum_{i=m}^{\infty} b_i t^i.$$

Without loss of generality, we may assume that $n = m$. Suppose sequences $(a_i)_{i=n}^{\infty}$ and $(b_i)_{i=n}^{\infty}$ are not equal, i.e. there is some j such that $a_j \neq b_j$. Assume that j is the minimal such number, then for any $k > j$

$$v_P\Big(\sum_{i=n}^{k} a_i t^i - \sum_{i=n}^{k} b_i t^i\Big) = v_P((a_j - b_j)t^j + \sum_{j+1}^{k}(a_i - b_i)t^i) = j.$$

But also,

$$\begin{aligned} v_P\Big(\sum_{i=n}^{k} a_i t^i - \sum_{i=n}^{k} b_i t^i\Big) &= v_P\Big(\sum_{i=n}^{k} a_i t^i + z - z - \sum_{i=n}^{k} b_i t^i\Big) \\ &\geq \min\Big\{v_P\Big(z - \sum_{i=n}^{k} a_i t^i\Big), v_P\Big(z - \sum_{i=n}^{k} b_i t^i\Big)\Big\}. \end{aligned}$$

In the expression above, as $k \to \infty$, $v_P\Big(\sum_{i=n}^{k} a_i t^i - \sum_{i=n}^{k} b_i t^i\Big)$ goes to infinity as well, contradicting the previous conclusion. Thus, the series representation is unique.

Now, consider a sequence $(c_i)_{i=n}^{\infty}$ in K. For all i, $v_P(c_i t^i) \geq i$, so the sequence $(c_i t^i)_{i=n}^{\infty}$ converges to 0. Consider the partial sum $s_k := \sum_n^k c_i t^i$. For $l > k$ we have

$$v_P(s_l - s_k) = v_P\Big(\sum_{i=k+1}^{l} c_i t^i\Big) \geq k + 1.$$

Hence $(s_i)_{i=n}^{\infty}$ is a Cauchy sequence and therefore converges in $\hat{F}_P$. So $\sum_n^{\infty} c_i t^i$ converges too, say to $y \in \hat{F}_P$. Let $j_0 := \min\{i \mid c_i \neq 0\}$. If $j_0 = \infty$, then $c_i = 0$ for all i and it follows that $y = 0$ and $v_P(y) = \infty$. If $j_0 < \infty$, then for all $k > j_0$

$$v_P\Big(\sum_{i=n}^{k} c_i t^i\Big) = j_0$$

and

$$v_P\Big(\sum_{i=n}^{k} c_i t^i\Big) > j_0.$$

Thus,

$$\begin{aligned} v_P(y) &= v_P\Big(y - \sum_{i=n}^{k} c_i t^i + \sum_{i=n}^{k} c_i t^i\Big) \\ &= \min\Big\{v_P\Big(y - \sum_{i=n}^{k} c_i t^i\Big), v_P\Big(\sum_{i=n}^{k} c_i t^i\Big)\Big\} = j_0. \end{aligned}$$

□

Definition 2.7. *Let M be a module over F. A mapping $\delta : F \to M$ is a derivation of F/K, if δ is K-linear and the product rule*

$$\delta(u \cdot v) = u \cdot \delta(v) + v \cdot \delta(u)$$

holds for all $u, v \in F$.

Lemma 2.8. *Let $\delta : F \to M$ be a derivation of F/K into M. Then we have:*

1. *$\delta(a) = 0$ for all $a \in K$.*
2. *$\delta(z^n) = nz^{n-1} \cdot \delta(z)$ for $z \in F$ and $n \geq 0$.*
3. *If char $K = p > 0$, then $\delta(z^p) = 0$ for each $z \in F$*
4. *$\delta(\frac{x}{y}) = \frac{y \cdot \delta(x) - x \cdot \delta(y)}{y^2}$ for $x, y \in F$ and $y \neq 0$*

Proof.

1. First consider $\delta(1)$:
$$\delta(1) = \delta(1^2) = \delta(1) + \delta(1).$$
It follows that $\delta(1) = 0$. Since δ is K-linear, for any $a \in K$ we have
$$\delta(a) = \delta(a \cdot 1) = a\delta(1) = 0.$$

2. Let $n = 2$, then
$$\delta(z^2) = 2z\delta(z).$$
By induction, it follows that for $n > 2$
$$\delta(z^n) = z\delta(z^{n-1}) + z^{n-1}\delta(z) = nz^{n-1}\delta(z).$$

3. By Part 2, we have
$$\delta(z^p) = pz^{p-1}\delta(z) = 0,$$
since *char* $F/K =$ *char* K.

4. $$\delta\left(\frac{x}{y}\right) = \delta(xy^{-1}) = y^{-1}\delta(x) - y^{-2}x\delta(y) = \frac{y\delta(x) + x\delta(y)}{y^2}.$$

□

Definition 2.9. *An element $x \in F$ is called a separating element for F/K if $F/K(x)$ is a finite separable extension.*

Definition 2.10. *Let t be a separating element of F/K. The unique derivation $\delta_t : F \to F$ with the property $\delta_t(t) = 1$ is called the derivation with respect to t.*

Lemma 2.11. *If x, y are a separating elements of F/K, then*

$$\delta_y = \delta_y(x) \cdot \delta_x$$

Lemma 2.12. *Suppose that t is a separating element of F/K and that $\delta_1, \delta_2 : F \to M$ are derivations of F/K and $\delta_1(t) = \delta_2(t)$. Then $\delta_1 = \delta_2$.*

Proof. (Claim 2.9.) Consider a polynomial $f(t) \in K[t]$. Using Lemma 1.6, we conclude

$$\delta_1(f(t)) = \sum \delta_1(a_i t^i) = \sum i a_i t^{i-1}\delta_1(t) = \sum i a_i t^{i-1}\delta_2(t) = \delta_2(f(t)).$$

Then for $\frac{f(t)}{g(t)} \in K(t)$ we have

$$\delta_1\Big(\frac{f(t)}{g(t)}\Big) = \frac{g(t)\delta_1(f(t)) - f(t)\delta_2(g(t))}{g(t)^2} = \frac{g(t)\delta_2(f(t)) - f(t)\delta_1(g(t))}{g(t)^2} = \delta_2\Big(\frac{f(t)}{g(t)}\Big).$$

Now, consider an arbitrary element $z \in F$ and let $h(x) \in K(t)[x]$ be its minimal polynomial.

$$0 = \delta_1(h(y)) = \delta_1\big(\sum u_i y^i\big) = \sum \big(u_i\delta_1(y^i) + y^i\delta_1(u_i)\big) \quad (4)$$

$$= \delta_1(y)\sum i u_i y^{i-1} + \sum y^i\delta(u_i). \quad (5)$$

Similar expression can be derived for $\delta_2(h(y))$. Since $F/K(t)$ is a separable extension, $h'(y) = \sum i u_i y^{i-1} \neq 0$. Therefore,

$$\delta_1(y) = -\frac{\sum y^i\delta_1(u_i)}{\sum i u_i y^{i-1}} = \delta_2(y).$$

□

Proof. (Lemma 2.8.) Since $\delta_y(x)\delta_x(x) = \delta_y(x)$, Claim 1.9 implies that $\delta_y = \delta_y(x)\cdot\delta_x$. □

Definition 2.13. *In the set $Z = \{(u,x) \in F \times F \mid x \text{ is separating}\}$ we define a relation $\sim$ by*

$$(u,x) \sim (v,y) \iff v = u \cdot \delta_y(x).$$

It is easy to see that $\sim$ to be an equivalence relation.

2. *We denote the equivalence class of $(u,x) \in Z$ with respect to the above equivalence relation by $u\ dx$ and call it a differential of F/K. We let*

$$\Delta_F = \{u\ dx \mid u,x \in F,\ x \text{ is separating}\}$$

be the set of all differentials.

Definition 2.14. *Suppose that P is a place of $F/\mathbb{F}_q$ of degree one and $t \in F$ is a P-prime element. If $z \in F$ has the P-adic expansion $z = \sum_{i=n}^{\infty} a_i t^i$ with $n \in \mathbb{Z}$ and $a_i \in \mathbb{F}_q$ we define its residue with respect to P and t by*

$$res_{P,t}(z) = a_{-1}.$$

For differential $\omega \in \Delta_F$, $\omega = u\ dt$, its residue is

$$res_P(\omega) = res_{P,t}(u)$$

The results of this section will be applied to prove one of the crucial results in Section 4.

3 Characters of order d over $\mathbb{F}_q[x]$

The material of this section is based on Chapter 3 of [Ros13]. But unlike Rosen, we will define the character to take value in μ_d, the set of d-th roots of unity in $\mathbb{C}^*$. We then fix an isomorphism Ω between μ_d and the d-th roots or unity in $\mathbb{F}_q^*$, assuming d divides $q-1$. Let $A = \mathbb{F}_q[x]$ be a polynomial ring over $\mathbb{F}_q$. We denote by $\mathcal{M}_q$ a set of all monic polynomials in A, by $\mathcal{M}_{q,n}$ the set of all monic polynomials of degree n. For $f \in A$, $f \neq 0$, we define its norm by

$$|f| = q^{\deg f}$$

If $f = 0$, we set $|f| = 0$.

Definition 3.1. *Let $P \in \mathbb{F}_q[x]$ be an irreducible polynomial and d as above. If $a \in \mathbb{F}_q[x]$ and P does not divide a, let $\left(\frac{a}{P}\right)_d$ be a unique element of μ_d such that if $a^{\frac{|P|-1}{d}} \equiv \alpha \mod P$, then*

$$\left(\frac{a}{P}\right)_d = \Omega^{-1}(\alpha).$$

If $P|a$, we set $\left(\frac{a}{P}\right)_d = 0$. The symbol $\left(\frac{a}{P}\right)_d$ is called the d-th residue symbol.

Proposition 3.2. *The cubic residue symbol has the following properties:*

1. $\left(\frac{a}{P}\right)_d \equiv \left(\frac{b}{P}\right)_d$ *if* $a \equiv b \mod P$
2. $\left(\frac{ab}{P}\right)_d = \left(\frac{a}{P}\right)_d \left(\frac{b}{P}\right)_d$
3. $\left(\frac{a}{P}\right)_d = 1$ *if and only if* $x^d \equiv a \mod P$ *has a solution*

Proof.

1. Follows from the definition.
2. Assume

$$a^{\frac{|P|-1}{d}} \equiv \alpha \mod P, b^{\frac{|P|-1}{d}} \equiv \beta \mod P.$$

Then

$$(ab)^{\frac{|P|-1}{d}} \equiv a^{\frac{|P|-1}{d}} b^{\frac{|P|-1}{d}} \mod P \equiv \alpha\beta \mod P.$$

Since $(ab)^{\frac{|P|-1}{d}}$ and $\alpha\beta$ are congruent modulo P and are constants, they must be equal. The result follows.

3. If $b^d \equiv a \mod P$, then $a^{\frac{|P|-1}{d}} \equiv b^{|P|-1} \equiv 1 \mod P$.
Let $A = \mathbb{F}_q[x]$. Suppose $a^{\frac{|P|-1}{d}} \equiv 1 \mod P$. Consider a homomorphism φ from $(A/PA)^*$ to itself such that $\varphi(a) = a^d$. Since $d||P|-1$, $x^d - 1$ divides $x^{|P|-1} - 1$. By Proposition 1.9 in *[R02]*, $x^{|P|-1} - 1$ splits as the product of distinct linear factors; hence, so is $x^d - 1$. Therefore, $x^d \equiv 1 \mod P$ has exactly d solutions in $(A/PA)^*$, so $\ker\varphi$ must be of order d. The image of φ is the set of all the powers of d -th and $|Im\ \varphi| = \frac{|P|-1}{d}$. Assume that $b^d \equiv 1 \mod P$. Then it must be a root of the equation $X^{\frac{|P|-1}{d}} - 1 = 0$. Therefore, all the d-th powers are exactly the roots of this equation and vice versa. Therefore, a is a d-th power as well.

□

Proposition 3.3. *Let $\alpha \in \mathbb{F}_q$. Then*

$$\left(\frac{\alpha}{P}\right)_d = \Omega(\alpha^{\frac{q-1}{d}\deg P})^{-1}$$

Proof.

$$\frac{q^{\deg P}-1}{d}=\frac{q-1}{d}(1+q+...+q^{\deg P-1})$$

The result follows since $\alpha^q=\alpha$. □

Theorem 3.4 (The d-th power reciprocity law.)**.** *Let P and Q be monic irreducible polynomials of degree n and m respectively. Then*

$$\left(\frac{Q}{P}\right)_d=(-1)^{\frac{q-1}{d}nm}\left(\frac{P}{Q}\right)_d$$

Proof. Define $\left(\frac{a}{P}\right):=\left(\frac{a}{P}\right)_{q-1}$. By definition, $\left(\frac{a}{P}\right)_d=\left(\frac{a}{P}\right)^{\frac{q-1}{d}}$. With this notation it suffices to prove that

$$\left(\frac{Q}{P}\right)=(-1)^{nm}\left(\frac{P}{Q}\right).$$

The main result follows by raising both sides to the power $(q-1)/d$.

Let α and β be the roots of P and Q respectively. Let $\mathbb{F}'$ be a finite field extension of $\mathbb{F}$ containing both α and β. Then

$$P(x)=\prod_{i=0}^{n-1}(x-\alpha^{q^i}),$$

$$Q(x)=\prod_{j=0}^{m-1}(x-\beta^{q^j}).$$

Note that for $f(x)\in\mathbb{F}'[x]$, we have $f(x)\equiv f(\alpha)\mod(x-\alpha)$. Also, if $g(x)\in A$, then $g(x)^q=g(x^q)$. From this, it follows that

$$\Omega\left(\left(\frac{Q}{P}\right)\right)\equiv Q(x)^{\frac{q^n-1}{q-1}}\equiv Q(x)^{1+q+...q^{n-1}}\equiv Q(\alpha)Q(\alpha^q)...Q(\alpha^{q^{n-1}})\mod(x-\alpha)$$

The congruence above holds modulo $(x-\alpha^{q^i})$ for all i, therefore it holds modulo P. Hence,

$$\Omega\left(\left(\frac{Q}{P}\right)\right)\equiv\prod_{i=0}^{n-1}\prod_{j=0}^{m-1}(\alpha^{q^i}-\beta^{q^j})\mod P.$$

Since both sides of the equation are in $\mathbb{F}'$, they should be equal. Therefore,

$$\left(\frac{Q}{P}\right)=\Omega^{-1}\left(\prod_{i=0}^{n-1}\prod_{j=0}^{m-1}(\alpha^{q^i}-\beta^{q^j})\right)=\Omega^{-1}\left((-1)^{nm}\prod_{i=0}^{n-1}\prod_{j=0}^{m-1}(\beta^{q^j}-\alpha^{q^i})\right)=(-1)^{nm}\left(\frac{P}{Q}\right).$$

□

We can extend the definition of the d -th power residue symbol to any monic polynomial in $\mathbb{F}_q[x]$. Let $g\in\mathbb{F}_q[x]$, $a\neq 0$, and $F=P_1^{e_1}...P_n^{e_n}$ be the prime decomposition of F. For $a\in\mathbb{F}_q[x]$, we define

$$\left(\frac{a}{F}\right)_d=\prod_{i=1}^{n}\left(\frac{a}{P_i}\right)_d^{e_i}. \tag{6}$$

With this definition, we can now formulate the reciprocity law for an arbitrary polynomial in $\mathbb{F}_q[x]$. For a non-zero $f \in \mathbb{F}_q[x]$, define $\mathrm{sgn}_d(f)$ to be the leading coefficient of f raised to power $\frac{q-1}{d}$.

Theorem 3.5 (The general reciprocity law)**.** *Let $a, b \in \mathbb{F}_q[x]$ be relatively prime, non-zero elements. Then,*

$$\Omega\Big(\Big(\frac{a}{b}\Big)_d \Big(\frac{b}{a}\Big)_d^{-1}\Big) = (-1)^{\frac{q-1}{d}\deg a \deg b} sgn_d(a)^{\deg b} sgn_d(b)^{-\deg a}$$

In particular, if $q \equiv 1 \mod 6$, then for $a, b \in \mathbb{F}_q[x]$ monic coprime non-zero polynomials, the reciprocity law is given by

$$\Big(\frac{a}{b}\Big)_3 = \Big(\frac{b}{a}\Big)_3$$

Proof. Let a, b be monic and irreducible, the theorem reduces to Theorem 3.4. Suppose $a = \alpha P_1^{e_1} \ldots P_n^{e_n}$ and $b = \beta Q_1^{f_1} \ldots Q_m^{f_m}$.. Using the definition of the character and Proposition 3.3, we have

$$\Omega\Big(\Big(\frac{a}{b}\Big)_d\Big) = \Omega\Big(\Big(\frac{\alpha}{b}\Big)_d \Big(\frac{P_1}{b}\Big)_d^{e_1} \ldots \Big(\frac{P_n}{b}\Big)_d^{e_n}\Big) = sgn_d(a)^{\deg b} \prod_{i=1}^{n} \prod_{j=1}^{m} \Omega\Big(\Big(\frac{P_i}{Q_j}\Big)_d^{e_i f_i}\Big).$$

Let δ_i and v_j denote the degree of P_i ad Q_j respectively. By Theorem 2.4,

$$\begin{aligned}
\Omega\Big(\Big(\frac{a}{b}\Big)_d\Big) &= sgn_d(a)^{\deg b} \prod_{i=1}^{n} \prod_{j=1}^{m} \Big[(-1)^{\frac{q-1}{d}\delta_i v_i} \Omega\Big(\Big(\frac{Q_j}{P_i}\Big)_d\Big)\Big]^{e_i f_i} \\
&= sgn_d(a)^{\deg b} (-1)^{\frac{q-1}{d}\deg a \deg b} \Omega\Big(\Big(\frac{\beta^{-1} b}{\prod_i P_i}\Big)_d\Big) \\
&= sgn_d(a)^{\deg b} sgn_d(b)^{\deg b} (-1)^{\frac{q-1}{d}\deg a \deg b} \Omega\Big(\Big(\frac{b}{a}\Big)_d\Big).
\end{aligned}$$

Multiplying both sides by $\Omega\Big(\Big(\frac{b}{a}\Big)_d^{-1}\Big)$ we arrive at the result. □

We are specifically interested in cubic characters, so from now on we assume that $d = 3$. We also want to fix a cubic character χ_3 on $\mathbb{F}_q^*$ by

$$\chi_3(\alpha) = \Omega^{-1}(\alpha^{\frac{q-1}{3}}). \tag{7}$$

For $d = 3$, we call the character primitive if and only if e_i in (5) is equal to either 1 or 2 for all i. Therefore, all conductors of cubic characters are monic square-free polynomials in $\mathbb{F}_q[x]$. Therefore, if we pick any conductor $F = F_1 F_2$ with $(F_1, F_2) = 1$, we have a primitive character modulo F given by

$$\Big(\frac{\alpha}{F_1 F_2^2}\Big)_3 = \Big(\frac{\alpha}{F_1}\Big)_3 \Big(\frac{\alpha}{F_2}\Big)_3^2 = \Big(\frac{\alpha}{F_1}\Big)_3 \overline{\Big(\frac{\alpha}{F_2}\Big)_3}$$

Thus, for each conductor F, there are $2^{\omega(F)}$ primitive characters, where $\omega(F)$ is the number of prime divisors of F.

4 Gauss sums

Before defining a Gauss sum, we must construct an additive character.

Building on the contents of Section 1 on function fields, we let F/K to be an algebraic function field and assume $K = \mathbb{F}_q$, where $q = p^m$ for some positive integer m. Then consider the completion of F with respect to v_∞, that is $\hat{F}_\infty = \mathbb{F}_q((x^{-1}))$, the field of all Laurent series in x^{-1}. Let $a \in \mathbb{F}_q$ and $e_q(a) = \exp\left(\frac{2\pi i \operatorname{tr}_{\mathbb{F}_q/\mathbb{F}_p}(a)}{p}\right)$. For $f \in \hat{F}_\infty$, define the function

$$e(f) = e_q(-\operatorname{res}_\infty(f dx)).$$

Since $f \in \hat{F}_\infty$, we can write $f(x) = \sum_{i=n}^{\infty} a_i \frac{1}{x^i}$ for some $n \in \mathbb{Z}$. We know that $t = \frac{1}{x}$ is the uniformizer of P_∞. Then

$$dx = -x^2 d\left(\frac{1}{x}\right).$$

Therefore,

$$f(x)dx = -x^2 f(x) d\left(\frac{1}{x}\right) = -\left[\sum_{i=n}^{\infty} a_i \left(\frac{1}{x}\right)^{i-2}\right] d\left(\frac{1}{x}\right).$$

Then, by definition of the residue,

$$-\operatorname{res}_\infty(f(x)dx) = a_1. \tag{8}$$

That is, $-\operatorname{res}_\infty(f(x)dx)$ is the coefficient of x^{-1} the Laurent expansion of f. Therefore, for $a, b \in \hat{F}_\infty$, $e(a+b) = e(a)e(b)$, and $e(g) = 1$ for $f \in \mathbb{F}_q[x]$. Also, if $a, b, h \in \mathbb{F}_q[x]$ and $a \equiv b \mod h$, then $e(\frac{a}{h}) = e(\frac{b}{h})$. Usually in the literature, the definition of the additive character does not go beyond a_1, that is, the formal definition involving the residue is not mentioned. There are considerable advantages in seeing the complete picture as we have presented it here, since now we will be able to see the additive character as a composition of an additive character over $\mathbb{F}_q$ and a trace of a suitable field extension. We will see more of it in the proof of Theorem 4.3.

Let $f, V \in \mathbb{F}_q[x]$. We define the generalized cubic Gauss sum by

$$G(V, f) = \sum_{a \mod f} \left(\frac{a}{f}\right)_3 e\left(\frac{aV}{f}\right)$$

Lemma 4.1. *Suppose that $q \equiv 1 \mod 6$.*

1. *If $h, f \in \mathbb{F}_q[x]$ are coprime, we have*

$$G(hV, f) = \left(\frac{h}{f}\right)_3^{-1} G(V, f)$$

2. *If $(f_1, f_2) = 1$, then*

$$G(V, f_1 f_2) = \left(\frac{f_1}{f_2}\right)_3^2 G(V, f_1) G(V, f_2) = \tag{9}$$

$$= G(V f_2, f_1) G(V, f_2) \tag{10}$$

3. If $V = V_1 P^\alpha$, where $P \nmid V_1$, then

$$G(V,P^i) = \begin{cases} 0 & \text{if } i \le \alpha \text{ and } i \not\equiv 0 \mod 3 \\ \phi(P^i) & \text{if } i \le \alpha \text{ and } i \equiv 0 \mod 3 \\ |P|^{i-1}\left(\frac{V}{P^i}\right)^{-1}\sum_{u \mod P}\left(\frac{u}{P^i}\right)_3 e\left(\frac{u}{P}\right) & \text{if } i = \alpha+1 \text{ and } i \not\equiv 0 \mod 3 \\ -|P|_q^{i-1} & \text{if } i = \alpha+1 \text{ and } i \equiv 0 \mod 3 \\ 0 & \text{if } i \ge \alpha+2 \end{cases} \tag{11}$$

Proof. Let A denote the ring of polynomials in x over $\mathbb{F}_q$. If h and f are coprime and if a runs over the entire set of representatives of A/fA, so does ah. Let $b = ah$, then it follows that

$$\begin{aligned} G(hV,f) &= \sum_{a \mod f}\left(\frac{a}{f}\right)_3 e\left(\frac{ahV}{f}\right) \\ &= \sum_{b \mod f}\left(\frac{bh^{-1}}{f}\right)_3 e\left(\frac{bV}{f}\right) = \left(\frac{h}{f}\right)_3^{-1} G(V,f) \end{aligned}$$

2.
$$G(V,f_1f_2) = \sum_{u \mod f_1f_2}\left(\frac{a}{f_1f_2}\right)_3 e\left(\frac{aV}{f_1f_2}\right).$$

Write $a \mod f_1f_2$ as $u = u_1f_1 + u_2f_2$, with $u_1 \mod f_2$ and $u_2 \mod f_1$.

$$\begin{aligned} G(V,f_1f_2) &= \sum_{u \mod f_1f_2}\left(\frac{u_1f_1+u_2f_2}{f_1f_2}\right)_3 e\left(\frac{(u_1f_1+u_2f_2)V}{f_1f_2}\right) \\ &= \sum_{u \mod f_1f_2}\left(\frac{u_1f_1}{f_2}\right)_3\left(\frac{u_2f_2}{f_1}\right)_3 e\left(\frac{u_1V}{f_2}\right)e\left(\frac{u_2V}{f_1}\right) \\ &= \left(\frac{f_1}{f_2}\right)\left(\frac{f_2}{f_1}\right)\sum_{u_1 \mod f_2}\sum_{u_2 \mod f_1}\left(\frac{u_1}{f_2}\right)_3\left(\frac{u_2}{f_1}\right)_3 e\left(\frac{u_1V}{f_2}\right)e\left(\frac{u_2V}{f_1}\right) \\ &= \left(\frac{f_1}{f_2}\right)^{-1} G(V,f_1)G(V,f_2). \end{aligned}$$

On the other hand, using the first part of the proposition, we have

$$\left(\frac{f_1}{f_2}\right)^{-1} G(V,f_1)G(V,f_2) = G(V,f_1f_2)G(V,f_2).$$

3. First, assume $i \le \alpha$. Then

$$G(V_1P^\alpha,P^i) = \sum_{a \mod P^i}\left(\frac{a}{P^i}\right)_3 e\left(V_1P^{\alpha-i}\right) = \sum_{a \mod P^i}\left(\frac{a}{P^i}\right)_3.$$

If $i \equiv 0 \mod 3$, then $\left(\frac{a}{P^i}\right) = 1$ if $(a,P) = 1$. It follows that in this case $G(V,P^i) = \Phi(P^i)$, where Φ is the Euler's totient function. If $i \not\equiv 0 \mod 3$, we have $G(V,P^i) = 0$ by orthogonality of characters. Next, let $i = \alpha+1$. We can write $a \mod P^i$ as $a = bP + c$ with $b \mod P^{i-1}$ and $c \mod P$. With this notation we rewrite the Gauss sum as

$$
\begin{aligned}
G(V,P)=&\sum_{b \mod P^{i-1}}\sum_{c \mod P}\Big(\frac{bP+c}{P^i}\Big)_3 e\big(\frac{(bP+c)V_1}{P}\big)\\
=&\sum_{b \mod P^{i-1}}\sum_{c \mod P}\Big(\frac{c}{P^i}\Big)_3 e\big(\frac{cV_1}{P}\big)\\
=&|P|^{i-1}\sum_{c \mod P}\Big(\frac{c}{P^i}\Big)_3 e\big(\frac{cV_1}{P}\big)
\end{aligned}
$$

Since $(V_1,P)=1$, cV_1 runs over the set of representatives $\mod P$, so we can write $u\equiv cV_1 \mod P$. Then

$$
G(V,P)=|P|^{i-1}\Big(\frac{V}{P^i}\Big)^{-1}\sum_{u \mod P}\Big(\frac{u}{P^i}\Big)_3 e\big(\frac{u}{P}\big).
$$

If $i\equiv 0 \mod 3$, then

$$
G(V,P)=|P|^{i-1}\Big(\frac{V}{P^i}\Big)^{-1}\sum_{u \mod P} e\big(\frac{u}{P}\big)=-|P|^{i-1}.
$$

□

To prove another crucial result about Gauss sums we need the Hasse-Davenport theorem.

Theorem 4.2 (Hasse-Davenport)**.** *. Let F be a finite field with q elements and F_s be a field such that $[F_s:F]=s$. Let χ,ψ be multiplicative and additive characters on F_s respectively. For $\alpha\in F$, let its norm $N_{F_s/F}(\alpha)$ be defined by*

$$
N_{F_s/F}(\alpha):=\alpha\cdot\alpha^q\cdot\ldots\cdot\alpha^{q^{s-1}}.
$$

Let χ' be a multiplicative character on F_s defined as a composition of χ and $N_{F_s/F}$:

$$
\chi'(\alpha)=\chi(N_{F_s/F}(\alpha)),
$$

and let ψ' be the additive character on F_s as the composition of the additive character ψ and $\mathrm{tr}_{F_s/F}$:

$$
\psi'(\alpha)=\psi(\mathrm{tr}_{F_s/F}(\alpha)).
$$

Let

$$
g(\chi,\psi)=\sum_{x\in F}\chi(x)\psi(s)
$$

be the Gauss sum over F, and $g(\chi',\psi')$ be the Gauss sum over F_s. Then

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

For any nontrivial character χ in $\mathbb{F}_q[x]$, we denote by $\tau(\chi)$ the Gauss sum of the restriction of χ to $\mathbb{F}_q^\times$, i.e.

$$
\tau(\chi)=\sum_{a\in\mathbb{F}_q^\times}\chi(a)e^{2\pi ia/p}
$$

If we treat A/fA, for $f\in A=\mathbb{F}_q[x]$ as an extension of degree $\deg f$ of $\mathbb{F}_q$, then we are able to apply this result to Gauss sums, as shown in the following theorem.

Theorem 4.3 (Theorem 2.1 in [Pat07]). *Let $V, f \in \mathbb{F}_q[x]$ be coprime. Then we have*

$$G(V,f) = \mu(V)\Big(\frac{-f}{V}\Big)_3^{-1}\Big(\frac{f'}{f}\Big)(-\tau(\chi_3))^{\deg f}$$

where f' denotes the derivative of f with respect to t.

Proof. By lemma 3.1, we know that if f is not square-free and is coprime to V, then $G(V,f) = 0$ and $\Big(\frac{f'}{f}\Big) = 0$, so we may assume f to be square-free. Since $(f, V) = 1$, we can use part 1 of the lemma 3.1 to write

$$G(V,f) = \Big(\frac{V}{f}\Big)_3^{-1} G(1,f).$$

Furthermore, if $f = f_1f_2$, then by part 3 of the lemma 3.1 we have

$$G(V,f_1f_2) = \Big(\frac{f_1}{f_2}\Big)_3^2 G(V,f_1)G(V,f_2).$$

Therefore, it is sufficient to prove the theorem for the case where $V = 1$ and f is irreducible. Then we have

$$G(1,f) = \sum_{a \mod f}\Big(\frac{a}{f}\Big)_3 e_q(-\mathrm{res}_\infty(\frac{a\ dx}{f})).$$

Since $df = f'dx$, we can rewrite the expression above as

$$G(1,f) = \sum_{a \mod f}\Big(\frac{a}{f}\Big)_3 e_q(-\mathrm{res}_\infty(\frac{a\ df}{f'f})).$$

Since f is irreducible, it must be coprime with f', so we can write $y \equiv c'a \mod c$ and thus factor out $\Big(\frac{f'}{f}\Big)_3$. Let $n = \deg f$, then we can identify $\mathbb{F}_q[x]/(f)$, where (f) is the maximal ideal of $\mathbb{F}_q[x]$, with $\mathbb{F}_{q^n}$. By Abel's Theorem, we have

$$\mathrm{res}_\infty(\frac{a\ df}{f}) = -\sum_{v \text{ finite}} \mathrm{res}_v(\frac{a\ df}{f}).$$

As f splits completely over $\mathbb{F}_{q^n}$, then $f = \prod_{i=1}^n (x-\alpha_i)$, and the sum in the expression above must be over all the zeros of f. Without loss of generality, consider the place associated to the polynomial $g_1(x) = x - \alpha_1$. Then we have

$$df = \Big(\prod_{i=1}^n (x-\alpha_i)\Big)' d(x-\alpha_1) = \Big(\prod_{i\neq 1}(x-\alpha_i)\Big) d(x-\alpha_1).$$

Also, notice that $a(x) = h(x)(x-\alpha_1) + a(\alpha_1)$ for some $h(x) \in \mathbb{F}_{q^n}[x]$. With this, we have that

$$\mathrm{res}_{x-\alpha_1}(\frac{a\ df}{f}) = \mathrm{res}_{x-\alpha_1}(\frac{a\ d(x-\alpha_1)}{x-\alpha_1}) = \mathrm{res}_{x-\alpha_1}((h(x) + \frac{a(\alpha_1)}{x-\alpha_1})\ d(x-\alpha_1)) = a(\alpha_1).$$

Thus,

$$\mathrm{res}_\infty(\frac{a\ df}{f}) = -\sum_{v \text{ finite}} \mathrm{res}_v(\frac{a\ df}{f}) = -\mathrm{tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(a).$$

Therefore, the additive character is given by $e(a) = \exp(\frac{2\pi i \operatorname{tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(a)}{q})$, i.e. the composition of the additive character on $\mathbb{F}_q$ and the trace. Finally, recall that $N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) := \alpha \cdot \alpha^q \cdot \ldots \cdot \alpha^{q^{s-1}} = \alpha^{\frac{q^n-1}{q-1}}$. Taking the composition of the multiplicative character on $\mathbb{F}_q$ and the norm, we get

$$\chi(N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(a)) = a^{\frac{q^n-1}{q-1} \cdot \frac{q-1}{3}} = \left(\frac{a}{f}\right)_3$$

for $a \in \mathbb{F}_q[x]/(f)$. The result follows directly from the Hasse-Davenport theorem. □

5 The Dirichlet series of Gauss sums

The material of this chapter is based on Chapters 3.1 and 3.2 of [DFL22]. Let $V \in \mathbb{F}_q[x]$ and $0 \leq i \leq 2$ and set $u = q^{-s}$ for $s \in \mathbb{C}$. Then we can define

$$\psi(V, i, u) = (1 - u^3 q^3)^{-1} \sum_{\substack{F \in \mathcal{M}_q \\ \deg F \equiv i \mod 3}} G(V, F) u^{\deg F}.$$

Notice that since $|G(V, F)| = q^{\deg F/2}$, this series converges for $\Re(s) > 3/2$, that is $|u| < q^{-3/2} < 1$.

Hoffstein proved in [Hof92] a functional equation for $\psi(V, i, u)$.

Theorem 5.1.

$$(1 - q^4 u^3)\psi(V, i, u) = |V|_q u^{\deg V} \Big[a_1(u)\psi(V, i, q^{-2}u^{-1}) + a_2(u)\psi(V, 1 + \deg V - i, q^{-2}u^{-1}) \Big],$$

where

$$a_1(u) = -(q^2 u)(qu)^{-[\deg V + 1 - 2i]_3}(1 - q^{-1}),$$
$$a_2(u) = -W_{V,i}(qu)^{-2}(1 - q^3 u^3),$$

with $W_{V,i} = \tau(\chi_3^{2i-1}\overline{\chi_V})$, *where* $\chi_V(a) = \left(\frac{a}{V}\right)_3$ *and* χ_3 *is given as in equation (7).*

The equation relates the values of the series at the points s and $s - 2$. Furthermore, Hoffstein also showed that by considering the behavior of both sides of the functional equation as $u \to \infty$, we can obtain that

$$\psi(V, i, u) = \frac{u^i P(V, i, u^3)}{1 - q^4 u^3}, \tag{12}$$

where $P(V, i, t)$ is a polynomial of degree at most $[(1 + \deg V - i)/3]$ in t. Thus, we are provided with an analytic continuation of the series beyond just $\Re(s) > 3/2$. In fact, we can see that the single pole of the series is the point $u = q^{-4/3}$, or $s = 4/3$.

We let

$$C(V, m) = \sum_{f \in \mathcal{M}_{q,m}} G(V, f). \tag{13}$$

Lemma 5.2. *Let* $n = [(1 + \deg V - i)/3]$, *then*

$$P(V, i, x) = \sum_{j=0}^{n} x^j \Big[C(V, i + 3j) + \sum_{k=0}^{j-1} C(V, i + 3k)(q^{3(j-k)}(1 - q)) \Big]. \tag{14}$$

Proof. Based on (12), we can write

$$P(V,i,x) = \frac{1-q^4x}{1-q^3x}\sum_{j\geq 0} C(V,i+3j)x^j.$$

Expanding $(1-q^3x)^{-1}$ as a series and grouping the coefficients by degree of x, we arrive at the result., we obtain:

$$\begin{aligned} P(V,i,x) &= (1-q^4x)\sum_{n\geq 0}(q^3x)^n \sum_{j\geq 0} C(V,i+3j)x^j \\ &= \sum_{j=0}^{\infty} x^j\Big[C(V,i+3j) + \sum_{k=0}^{j-1} C(V,i+3k)(q^{3(j-k)}(1-q))\Big] \end{aligned}$$

Based on the work of Hoffstein, $P(V,i,x)$ is of degree at most $[(1+\deg V - i)/3]$. Applying this to the expression above, the result follows. □

Definition 5.3. *Assume $V \in \mathbb{F}_q[x],\ 0 \leq i \leq 2$. Let*

$$\rho(V,i) = \lim_{s\to 1+\frac{1}{3}} (1-q^{3+1-ns})q^{is}\psi(V,i,q^{-s})) = P(V,i,q^{-3-1}).$$

Proposition 5.4 (Lemma 3.9 in [DFL22])**.** *Let $V = V_1V_2^2V_3^3$ with V_1, V_2 square-free and $(V_1,V_2) = 1$. If $V_2 \neq 1$, then $\rho(V,i) = 0$. Otherwise, we have*

$$\rho(V,i) = \overline{G(1,V_1)}|V_1|^{-2/3}q^{\frac{4}{3}i-\frac{4}{3}[i-2\deg V]_3}\rho(1,[i-2\deg V]_3)$$

with

$$\rho(1,0) = 1,\ \rho(1,1) = \tau q,\ \rho(1,2) = 0.$$

Theorem 5.5 ([DFL22])**.** *For $V \in \mathbb{F}_q[x],\ m \in \mathbb{Z}^+$, we have*

$$C(V,m) = Aq^{4m/3} + O(|r|^{1/4}q^{m(1+\epsilon)},)$$

where $A = \frac{(1-q^{-1})\rho(V,i)}{q^{-4i/3}}$ and $m \equiv i \mod 3$.

The rest of the section is dedicated to proving Proposition 5.4. To do so we will need a number of auxiliary lemmas. First, for a prime π, we define

$$\psi_\pi(V,i,u) = (1-q^3u^3)^{-1} \sum_{\substack{F\in\mathcal{M}_q \\ \deg F\equiv i \mod 3 \\ (F,\pi)=1}} G(V,F)u^{\deg f}$$

Lemma 5.6. *Let π be a prime that does not divide V. Then we have*

$$\psi_\pi(V,i,u) = \psi(V,i,u) - G(V,\pi)|\pi|_q^{-s}\psi_\pi(V\pi, i-\deg\pi, u),$$

$$\psi_\pi(V\pi,i,u) = \psi_\pi(V\pi,i,u) - \overline{G(V,\pi)}|\pi|_q^{1-2s}\psi_\pi(V, i-2\deg\pi, u),$$
$$\psi_\pi(V\pi^2,i,u) = (1-|\pi|^{2-3s})^{-1}\psi(f\pi^2,i,q^{-s}).$$

Proof. By definition,

$$\psi_\pi(V,i,u) = \psi(V,i,u) - (1-q^3u^3)^{-1} \sum_{\substack{F\in\mathcal{M}_q \\ \deg F\equiv i \mod 3 \\ (F,\pi)\neq 1}} G(V,F).$$

Considering that $(\pi, V) = 1$, we have $G(f,F) \neq 0$ if and only if $F = \pi F_1$, where π does not divide F_1. Then, using Lemma 3.1 to split a Gauss sum into a product, we obtain

$$\begin{aligned}
&\sum_{\substack{F_1\in\mathcal{M}_q \\ \deg F_1\equiv i-\deg\pi \mod 3 \\ (F_1,\pi)=1}} G(V,\pi F_1)u^{\deg\pi+\deg F_1} \\
&\qquad = G(V,\pi)u^{\deg\pi} \sum_{\substack{F\in\mathcal{M}_q \\ \deg F\equiv i-\deg\pi \mod 3 \\ (F_1,\pi)=1}} G(V\pi,F_1)u^{\deg F_1}.
\end{aligned}$$

Putting the equations above together, the first relation follows. The proofs of the other two identities proceed in a similar fashion. □

Lemma 5.7. *Let π be a prime that does not divide V. Then we have*

$$\psi(V\pi^{j+3},i,u) - |\pi|^{3(1-s)}\psi(V\pi^j,\pi_\infty^{-i},u) = (1-|\pi|^{2-3s})\psi_\pi(V\pi^j,i,u)$$

Proof. Write

$$\begin{aligned}
\sum_{\deg F\equiv i \mod 3} \frac{G(V\pi^j,F)}{|F|^s} &= \sum_{\substack{\deg F\equiv i(3) \\ (F,\pi)=1}} \frac{G(V\pi^j,F)}{|F|^s} + \sum_{l=1}^{\lfloor\frac{j}{3}\rfloor} |\pi|^{-3ls} \sum_{\substack{\deg F\equiv i \mod 3 \\ (F,\pi)=1}} \frac{G(V\pi^j,\pi^{3l}F)}{|F|^s} \\
&\quad + |\pi|^{-(j+1)s} \sum_{\substack{\deg F\equiv i-(j+1)\deg\pi \mod 3 \\ (F,\pi)=1}} \frac{G(V\pi^j,\pi^{j+1}F)}{|F|^s}.
\end{aligned}$$

Notice that if $(F,\pi) = 1$ and $k = 3m + [k]_3$, then, using properties of Gauss sums, $G(V\pi^k,F) = \left(\frac{\pi^{3m}}{F}\right)_3 G(V\pi^{[k]_3},F)$. By Lemma 3.1.3,

$$G(V\pi^k,\pi^{3l}F) = G(V\pi^{j+3l},F)G(V\pi^j,\pi^{3l}) = G(V\pi^j,F)\phi(\pi^{3l}).$$

Observe that

$$G(V\pi^j,\pi^{j+1}) = \sum_{a \mod \pi^{j-[j]_3}} \sum_{r \mod \pi^{[j]_3+1}} \left(\frac{r}{\pi^{[j]_3+1}}\right)_3 e\left(\frac{rV}{\pi}\right) = |\pi|^{j-[j]_3} G(V\pi^{[j]_3},\pi^{[j]_3+1}).$$

It follows that

$$\begin{aligned}
G(V\pi^j,\pi^{j+1}F) &= G(V\pi^{2j+1},F)G(V\pi^j,\pi^{j+1}) \\
&= G(V\pi^{2[j]_3+1},F)G(V\pi^{[j]_3},\pi^{[j]_3+1})|\pi|^{j-[j]_3} \\
&= G(V\pi^{[j]_3},\pi^{[j]_3+1}F)|\pi|^{j-[j]_3}.
\end{aligned}$$

Using these relations, we can rewrite the Gauss sum as follows:

$$\sum_{\deg F\equiv i \mod 3} \frac{G(V\pi^j,F)}{|F|^s} = \left(1+\sum_{l=1}^{j/3}\frac{\phi(\pi^{3l})}{|\pi|^{3ls}}\right) \sum_{\substack{\deg F\equiv i \mod 3\\ (F,\pi)=1}} \frac{G(V\pi^j,F)}{|F|^s}$$

$$+|\pi|^{(j-[j]_3)(1-s)} \sum_{\substack{\deg F\equiv i \mod 3\\ \pi|F}} \frac{G(V\pi^{[j]_3},F)}{|F|^s},$$

where the second summand is derived through the following process

$$|\pi|^{-(j+1)s} \sum_{\substack{\deg F\equiv i-(j+1)\deg\pi \mod 3\\ (F,\pi)=1}} \frac{G(V\pi^j,\pi^{j+1}F)}{|F|^s}$$

$$= |\pi|^{-(j+1)s+j-[j]_3} \sum_{\substack{\deg F\equiv i-(j+1)\deg\pi \mod 3\\ (F,\pi)=1}} \frac{G(V\pi^{[j]_3},\pi^{[j]_3+1}F)}{|F|^s}$$

$$= |\pi|^{-(j+1)s+j-[j]_3} \sum_{\substack{\deg F\equiv i \mod 3\\ \pi|F}} \frac{G(V\pi^{[j]_3},F)}{|F|^s}\pi^{s([j]_3+1)}$$

$$= |\pi|^{(j-[j]_3)(1-s)} \sum_{\substack{\deg F\equiv i \mod 3\\ \pi|F}} \frac{G(V\pi^{[j]_3},F)}{|F|^s}.$$

Repeating the procedure for $j+3$, we find that

$$\sum_{\deg F\equiv i \mod 3} \frac{G(V\pi^{j+3},F)}{|F|^s} = \pi^{(1-s)(j-[j]_3+3)} \sum_{\substack{\pi|F\\ \deg F\equiv i \mod 3}} \frac{G(V\pi^j,F)}{|F|^s}$$

$$+\left(1+\sum_{l=1}^{[j/3]+1}\frac{\phi(\pi^{3l})}{|\pi|^{3ls}}\right)\sum_{(F,\pi)=1}\frac{G(V\pi^j,F)}{|F|^s}.$$

We also have

$$|\pi|^{3-3s}\left(1+\sum_{l=1}^{[j/3]}\frac{\phi(\pi^{3l})}{|\pi|^{3ls}}\right) = \frac{(1-|\pi|)|\pi|^{-3s([j/3]+1)+j-[j]_3+5}-|\pi|^{5-3s}+|\pi|^3}{|\pi|^{3s}-|\pi|^3}$$

$$= |\pi|^{2-3s} - \frac{(|\pi|-1)|\pi|^{2-3s([j/3]+2)}\left(|\pi|^{3s([j/3]+2)}-|\pi|^{3([j/3]+s+1)}\right)}{|\pi|^{3s}-|\pi|^3}$$

$$= |\pi|^{2-3s} - \sum_{l=1}^{[j/3]+1}\frac{\phi(\pi^{3l})}{|\pi|^{3ls}}$$

Putting everything together, we arrive at

$$\sum_{\deg F\equiv i \mod 3} \frac{G(V\pi^{j+3},F)}{|F|^s} - |\pi|^{3-3s} \sum_{\deg F\equiv i \mod 3} \frac{G(V\pi^j,F)}{|F|^s}$$

$$= (1-|\pi|^{2-3s}) \sum_{\substack{\deg F\equiv i \mod 3\\ (F,\pi)=1}} \frac{G(V\pi^j,F)}{|F|^s}.$$

Multiply both sides by $(1 - q^{3(1-s)})$ to obtain the result. $\square$

We will be using the following result from the theory of metaplectic forms, as given [KP84], p.134.

Theorem 5.8 (Periodicity theorem)**.** *Let π be a prime that does not divide V. Then*

$$\rho(f\pi^{j+3}, i) = \rho(f\pi^j, i)$$

Lemma 5.9. *Let π be a prime that does not divide V. Then we have*

$$\lim_{s\to 4/3} q^{is}(1 - q^{4-3s})\psi_\pi(V\pi^j, i, u) = \frac{\rho(f\pi^j, i)}{1 + |\pi|^{-1}}.$$

Proof. Multiply the relation from Lemma 4.4 by $q^{is}(1 - q^{4-3s})$ and take the limit as $s \to 4/3$. Then, by definition,

$$\rho(V\pi^{j+3}, i) - |\pi|^{-1}\rho(V\pi^j, i) = (1 - |\pi|^{-2}) \lim_{s\to 4/3} q^{is}(1 - q^{4-3s})\psi_\pi(V\pi^j, \pi^{-i}, u).$$

The result follows from the Periodicity Theorem. $\square$

With all the necessary results at our disposal, we can finally prove Proposition 5.4.

*Proof. (Proposition 5.4.)*Remember from the definition,

$$\rho(V, i) = \lim_{s\to 4/3}(1 - q^{4-3s})q^{is}\psi(V, \pi_\infty^{-i}, q^{-s}).$$

First, we will compute $\rho(1, [i]_3)$,so we set $f = 1$ in the definition. Recall that

$$\begin{aligned} G(1, F) &= \sum_{a \mod F} \left(\frac{a}{F}\right)_3 e\left(\frac{a}{F}\right) = \sum_{\deg a \le \deg F-2} \left(\frac{a}{F}\right)_3 + \sum_{\deg a = \deg F-1} \left(\frac{a}{F}\right)_3 e\left(\frac{a}{V}\right) \\ &= \sum_{c\in\mathbb{F}_q^*} \sum_{\deg u \le \deg F-2} \left(\frac{c}{F}\right)_3 \left(\frac{u}{F}\right)_3 + \sum_{c\in\mathbb{F}_q^*} \sum_{u\in\mathcal{M}_{q,\deg F-1}} \left(\frac{c}{F}\right)_3 \left(\frac{u}{F}\right)_3 e^{2\pi i \operatorname{tr}_{\mathbb{F}_q/\mathbb{F}_p}(c)/p} \\ &= \sum_{c\in\mathbb{F}_q^*} \left(\frac{c}{F}\right)_3 \sum_{\deg u \le \deg F-2} \left(\frac{u}{F}\right)_3 + \tau(\chi_F) \sum_{u\in\mathcal{M}_{q,\deg F-1}} \left(\frac{u}{F}\right)_3, \end{aligned}$$

where $\tau(\chi_F) = \sum_{c\in\mathbb{F}_q^*} \left(\frac{c}{f}\right)_3 e^{2\pi i \operatorname{tr}_{\mathbb{F}_q/\mathbb{F}_p}(c)/p}$, i.e. the restriction of the Gauss sum to the units in $\mathbb{F}_q$. Assume that $[i]_3 = 0$, so that we must consider only F such that $\deg F \equiv 0 \mod 3$. Therefore, the character is trivial on $\mathbb{F}_q^*$ and

$$\sum_{a\in\mathcal{M}_{q,\le \deg F-1}} \left(\frac{a}{F}\right)_3 = \frac{\phi(F)}{q-1}$$

if F is a cube and vanishes otherwise. Let $\delta(F) = 1$ if F is a cube and 0 otherwise. Now, we can write

$$\begin{aligned} G(1, f) &= \sum_{c\in\mathbb{F}_q^*} \left(\frac{c}{F}\right)_3 \Big(\sum_{\deg u \le \deg F-1} \left(\frac{u}{F}\right)_3 - \sum_{u\in\mathcal{M}_{q,\deg F-1}} \left(\frac{u}{F}\right)_3 \Big) + \tau(\chi_F) \sum_{u\in\mathcal{M}_{q,\deg F-1}} \left(\frac{u}{F}\right)_3 \\ &= \phi(F)\delta(F) + q \sum_{u\in\mathcal{M}_{q,\deg F-1}} \left(\frac{u}{F}\right)_3. \end{aligned}$$

The result above follows from the fact that if $[i]_3 = 0$, then $\tau(\chi_F) = -1$ and $\sum_{c\in\mathbb{F}_q^*}\left(\frac{c}{F}\right) = q-1$. FInally, we arrive at

$$\begin{aligned}
\psi(1,0,u) &= (1-q^3u^3)^{-1} \sum_{\substack{F\in\mathcal{M}_q \\ \deg F\equiv 0 \mod 3}} G(1,F)u^{\deg F} \\
&= (1-q^3u^3)^{-1}\Big[\sum_{\substack{F=a^3 \\ a\in\mathcal{M}_q}} \phi(F)u^{\deg F} - q \sum_{\substack{F\in\mathcal{M}_q \\ \deg F\equiv 0 \mod 3}} \sum_{v\in\mathcal{M}_{q,\deg F-1}} \left(\frac{v}{F}\right)_3 u^{\deg F}\Big] \\
&= (1-q^3u^3)^{-1}\Big[\sum_{\substack{F=a^3 \\ a\in\mathcal{M}_q}} \phi(F)u^{\deg F} - q \sum_{v\in\mathcal{M}_{q,\deg F-1}} \sum_{\substack{F\in\mathcal{M}_q \\ \deg F\equiv 0 \mod 3}} \left(\frac{F}{v}\right)_3 u^{\deg F}\Big] \\
&= (1-q^3u^3)^{-1}\Big[\sum_{\substack{F=a^3 \\ a\in\mathcal{M}_q}} \phi(F)u^{\deg F} - q^{k+1}\#\{v\in\mathcal{M}_{q,\deg F-1} \mid v \text{ is a cube}\}\Big]
\end{aligned}$$

Since $3|\deg F$, $\#\{v\in\mathcal{M}_{q,\deg F-1} \mid v \text{ is a cube}\} = 0$.

Another fact that we will be using is, as shown in Proposition 2.7 in [Ros13],

$$\sum_{f\in\mathcal{M}_{q,n}} \phi(f) = q^{2n}(1-q^{-1}).$$

Therefore,

$$\begin{aligned}
\psi(1,0,u) &= (1-q^3u^3)^{-1} \sum_{f\in\mathcal{M}_q} \phi(f^3)u^{3\deg f} \\
&= (1-q^3u^3)^{-1} \sum_{k=0}^{\infty} \sum_{f\in\mathcal{M}_{q,k}} \phi(f)|f|^2 u^{3\deg f} \\
&= (1-q^3u^3)^{-1} \sum_{k=0}^{\infty} q^{4k}(1-q^{-1})u^{3k} \\
&= \frac{(1-q^{-1})}{(1-q^3u^3)(1-q^4u^3)}.
\end{aligned}$$

Taking the residue, we conclude that

$$\rho(1,0) = 1.$$

Now, suppose that $[i]_3 \neq 0$. Then $\sum_{c\in\mathbb{F}_q^*}\left(\frac{c}{F}\right) = 0$ and therefore

$$\begin{aligned}
\psi(1,i,u) &= (1-q^3u^3)^{-1} \sum_{\substack{F\in\mathcal{M}_q \\ \deg F\equiv i \mod 3}} G(1,F)u^{\deg F} \\
&= (1-q^3u^3)^{-1} \sum_{\substack{F\in\mathcal{M}_q \\ \deg F\equiv i \mod 3}} \tau(\chi_F) \sum_{u\in\mathcal{M}_{q,\deg F-1}} \left(\frac{u}{F}\right)_3 u^{\deg F} \\
&= (1-q^3u^3)^{-1}\tau(\chi_3^i) \sum_{\substack{F\in\mathcal{M}_q \\ \deg F\equiv i \mod 3}} \sum_{u\in\mathcal{M}_{q,\deg F-1}} \left(\frac{u}{F}\right)_3 u^{\deg F}.
\end{aligned}$$

If $[i]_3 = 1$, then

$$\begin{aligned}\psi(1,1,u) &= (1-q^3u^3)^{-1}\tau(\chi_3)\sum_{v\in\mathcal{M}_{q,3j}}\sum_{F\in\mathcal{M}_{q,3j+1}}\left(\frac{F}{v}\right)_3\\ &= (1-q^3u^3)^{-1}\tau(\chi_3)\sum_{j=0}^{\infty}u^{3j+1}q^{3j+1}\sum_{u\in\mathcal{M}_{q,j}}\frac{\phi(u^3)}{|u^3|}\\ &= (1-q^3u^3)^{-1}\tau(\chi_3)\sum_{j=0}^{\infty}u^{3j+1}q^{3j+1}q^j(1-q^{-1})\\ &= \frac{\tau(\chi_3)(q-1)u}{(1-q^3u^3)}\sum_{j=0}^{\infty}u^{3j}q^{4j}\\ &= \frac{\tau(\chi_3)(q-1)u}{(1-q^3u^3)(1-q^4u^3)}.\end{aligned}$$

Taking the residue, we get

$$\rho(1,1) = \tau(\chi_3)q.$$

Finally, if we have $[i]_3 = 2$, then, as in the case of $[i]_3 = 0$, there are obviously no cubes of degree congruent to $1 \mod 3$. It follows that

$$\rho(1,2) = 0.$$

Now, we can move to proving the main part of the lemma. We start with the following relation from Lemma 5.6:

$$\psi_\pi(V\pi,i,u) = \psi_\pi(V\pi,i,u) - \overline{G(V,\pi)}|\pi|_q^{1-2s}\psi_\pi(V,i-2\deg\pi,u),$$

Multiply its both sides by $q^{is(1-q^4u^3)}$ and take a limit as $s\to 4/3$. Using Lemma 5.9, we obtain

$$\rho(V\pi,i)\Big[1-\frac{1}{1+|\pi|^{-1}}\Big] = \overline{G(V,\pi)}|\pi|_q^{-5/3}q^{8\deg\pi/3}\frac{\rho(V,i-2\deg\pi)}{1+|\pi|^{-1}}.$$

We multiply both sides by $\frac{|\pi|}{1+|\pi|^{-1}}$ to get

$$\rho(V\pi,i) = \overline{G(V,\pi)}|\pi|_q^{-2/3}q^{8\deg\pi/3}\frac{\rho(V,i-2\deg\pi)}{1+|\pi|^{-1}}.$$

We repeat the procedure with equation

$$\psi_\pi(V\pi^2,i,u) = (1-|\pi|^{2-3s})^{-1}\psi(f\pi^2,\pi_\infty^{-i},q^{-s})$$

and obtain

$$\rho(V\pi^2,i) = \frac{1-|\pi|^{-2}}{1+|\pi|^{-1}}\rho(V\pi^2,i).$$

It follows from the relation above that $\rho(V\pi^2,i) = 0$. Therefore, we can assume from now on that V is square-free. Furthermore, as we have seen in Lemma 5.6, $\rho(V,i)$ depends only on the cubic-free part of V. So we can assume that $V = \pi_1...\pi_n$. Using previous results, we have

$$\rho(V,i) = \overline{G(V/\pi_1,\pi_1)}|\pi|_q^{-2/3}q^{8\deg\pi_1/3}\rho(V/\pi_1,i-2\deg\pi_1).$$

Notice that

$$
\begin{aligned}
q^{\frac{8}{3}\deg\pi}\rho(f,i-2\deg\pi) &= \lim_{s\to 4/3}(1-q^4u^3)q^{is}\psi(f,\pi^{-[i-2\deg\pi]_3},u) \\
&= \rho(f,[i-2\deg\pi]_3)q^{\frac{4}{3}(i-[i-2\deg\pi]_3)}.
\end{aligned}
$$

Substitute it into the previous relation and proceed

$$
\begin{aligned}
\rho(V,i) &= \overline{G(V/\pi_1,\pi_1)}|\pi_1|_q^{-2/3}q^{\frac{4}{3}(i-[i-2\deg\pi_1]_3)}\rho(V/\pi_1,[i-2\deg\pi_1]_3) \\
&= \overline{G(\frac{V}{\pi_1},\pi_1)}|\pi_1\pi_2|_q^{-2/3}q^{\frac{4}{3}[i-2(\deg\pi_1+\deg\pi_2)]_3}\cdot\overline{G(\frac{V}{\pi_1\pi_2},\pi_2)} \\
&\quad\cdot\rho(\frac{V}{\pi_1\pi_2},[i-2(\deg\pi_1+\deg\pi_2)]_3) \\
&= \ldots \\
&= \prod_{j=1}^{n}\overline{G\Big(\prod_{l=1}^{j-1}\pi_l,\pi_j\Big)}|V|^{-2/3}q^{\frac{4}{3}(i-[i-2\deg V]_3)}\rho(1,[i-2\deg V]_3).
\end{aligned}
$$

By Lemma 3.1,

$$
\prod_{j=1}^{n}\overline{G\Big(\prod_{l=1}^{j-1}\pi_l,\pi_j\Big)}=\overline{G(1,V)}.
$$

This finishes the proof. □

6 Algorithm and Computations

In this section, we take a closer look at each component of the computation separately and explain approach.

6.1 Multiplicative character.

There are two possible was to approach the multiplicative character. The first one is the exponentiation. Recall that, by definition,

$$
\left(\frac{a}{P}\right)_d \equiv a^{\frac{|P|-1}{d}} \mod P.
$$

Considering how fast $\frac{|P|-1}{d}$ grows, even when using fast exponentiation methods, such as exponentiation by squaring, it would still take too long, since we are still to use polynomial multiplication.

So, as in the case with number fields, we opt for using cubic reciprocity, which proves to be far more efficient. It would take at most n steps to evaluate $\left(\frac{a}{b}\right)_3$,where $n=\max(\deg a,\deg b)$. Each step would involve division. When using long division, the complexity of the method is $O(n^3)$.

6.2 Additive character.

When we are computing $e\left(\frac{ar}{c}\right)$, the main challenge is finding the coefficient a_1 of T^{-1} in the Laurent expansion of $\frac{ar}{c}$, that is, $\mathrm{res}_\infty\left(\frac{ar}{c}\right)$, as we earlier explained. The direct approach requires a multiplication and a division of polynomials. The naive multiplication of both has a time complexity of $O(n^2)$, where n is the degree of the polynomials. Using the Fast Fourier Transform (FFT) for a sped up polynomial multiplication, it can be improved at best to $O(n \log n)$.

Instead, we choose to treat it as a linear function. In a Gauss sum $G(r, c)$ we have the shift V and the conductor f fixed. Write $a(t) = a_0 + a_1 t + ... + a_n t^n$. Then

$$\text{res}_\infty(\frac{ar}{c}dt) = \sum_{i=0}^{n} a_i \text{res}_\infty(\frac{t^i r}{c}dt).$$

For a fixed pair r, c, $\text{res}_\infty(\frac{t^i r}{c}dt)$ are all fixed as well, so they can be computed and then retrieved upon need from memory for the computation of the Gauss sum $G(r, c)$. It changes the complexity from quadratic to linear, as polynomials $a \mod c$ can be be viewed as vectors.

6.3 Gauss sum.

As we pointed out in the introduction, a straightforward implementation would have the complexity of $O(q^n)$, where n is the degree of a conductor of the Gauss sum. In the early stages of the project, we had been practicing this naive approach, but very quickly faced technical difficulties. The computation of a single polynomial $P(V, i, u^3)$ for $\deg V = 5$ and $i = 1$ would take several hours of running time on an average desktop computer, making it impossible to gather enough data in a reasonable time frame even just for linear cases. Hence, we had to walk away from this and search for a different approach.

Hence, we in our computations we will apply a far more efficient tool, that is Theorem 3.3. Recall that for $V, f \in \mathbb{F}_q[x]$ coprime, we have

$$G(V, f) = \mu(f)\Big(\frac{-V}{f}\Big)_3^{-1}\Big(\frac{f'}{f}\Big)(-\tau(\chi))^{\deg f}.$$

This relation allows to completely avoid the lengthy summation and evaluation of characters at every step. Also, notice that most of the components on the right-hand side depend only on f. Therefore, we can further accelerate the process at the cost of memory by precomputing and storing the values of $\mu(f)\Big(\frac{f'}{f}\Big)(-\tau(\chi))^{\deg f}$. This reduces the computation of a Gauss sum to a single evaluation of the cubic character $\Big(\frac{-V}{f}\Big)_3^{-1}$ and a multiplication.

The main drawback of the method is that it requires the conductor and the shift to be coprime. It works best when the shift V is an irreducible polynomial. When it is not, most of the time there is still a number of cases, which grows exponentially with the size of the input, that requires a different approach.

We handle the non-coprime cases by using Lemma 4.1.2 and splitting a Gauss sum into a product based on the factorization of both the conductor and the shift. Then we can evaluate them separately, using either Lemma 4.1.3 or Theorem 4.3.

Due to this limitation, we still have to deal with a rapidly increasing number of computationally challenging cases as the size of the input grows, unless we limit our consideration to solely irreducible polynomials.

Elaborating on the method used to compute the additive character, we can also rewrite the Gauss sum as

$$\sum_{a_n=0}^{q-1} \sum_{a_{n-1}=0}^{q-1} \dots \sum_{a_0=0}^{q-1} \chi_f(a_0, \dots, a_{n-1}, a_n) e^{-\frac{2\pi i}{q}(a_0 K_0 + \dots + a_{n-1} K_{n-1} + a_n K_n)}.$$

Here $\chi_f(a_0, \dots, a_{n-1}, a_n) = \left(\frac{a_n x^n + \dots + a_0}{f}\right)_3$ and $K_i = \mathrm{res}_\infty(\frac{t^i r}{c} dt)$. One can notice that when presented in this form, the Gauss sum can be treated as a multidimensional Fourier transform. Therefore, we can evaluate a Gauss sum via FFT. It proves to be very efficient when used for non-coprime shift and conductor, specifically when they fall under the fourth case in Lemma 3.1.

Now we are able to rearrange $C(r, m)$ with regard to Theorem 3.3. Define

$$C^*(r, m) = \sum_{\substack{c \in \mathcal{M}_{q,m} \\ (r,c)=1}} G(r, c).$$

We can write $c = r^* c_1$ in $C(r, m)$, with $(r^*, c_1) = 1$, where $r^* | r^\infty$, i.e. r^* divides some power of r. Then

$$C(r, m) = \sum_{\substack{r^* \\ \deg r^* \leq m}} G(r, r^*) C^*(r r^*, m - \deg r^*).$$

By definition, we can use Theorem 3.3 when computing C^*. Note that, by Lemma 3.1, when r is square-free the only possibility for r^*, for which $G(r, r^*) \neq 0$, is $r^* = r^2$.

6.4 Residue.

There are three ways we can make use of Proposition 5.4. First, as we have said before, we use it to filter out polynomial inputs that are guaranteed to yield a trivial zero of $P(V, i, x)$.

Second, it can be utilized as a sanity check, as it provides the value of the polynomial P at the point q^{-4}. Then we can compare it to the obtained polynomial evaluated at that point to verify the validity of the computation.

Last, using interpolation, we can avoid computing one of the coefficients. The size and hence the complexity of computation of $C(V, m)$ depends mainly on the size of m, as it defines the set of polynomials over which we are summing. The sums appearing in the coefficients of $P(V, i, u^3)$ are all of the form $C(V, i + 3j)$, where $0 \leq j \leq \deg P$. Note that $C(V, 3 + m)$, by definition, requires up to q^3 times more operations to compute than $C(V, m)$. Thus, every subsequent $C(V, i + 3j)$ becomes a bigger computational challenge and the leading coefficient of $P(V, i, u^3)$ would take the longest to evaluate. Suppose $\deg P = n$, then, by definition of $\rho(f, i)$, we have

$$\rho(V, i) = c_n q^{-4n} + \dots + c_1 q^{-4} + c_0.$$

Assume that we know all the coefficients c_i, $0 \leq i \leq n - 1$. The exact value of $\rho(V, i)$ is given by Lemma 4.1 and does not require a computation as extensive as any of $C(V, m)$. Then, obviously,

$$c_n = q^{4n}(\rho(V, i) - (c_0 + c_1 q^{-4} + \dots + c_{n-1} q^{-4(n-1)}).$$

For linear $P(V, i, u^3)$ we used the residue to validate the computation, since the running time required to process a single polynomial was still relatively low. To keep the running time practically the same as in linear polynomials, for quadratic $P(V, i, u^3)$ we switch to using the residue as a computational tool by means of interpolation.

6.5 Technical.

All the code was written in python and is available upon the request. We also used functions *fft.fftn* and *roots* from the numpy package for computing FFT and finding roots respectively. The algorithm in its current state heavily relies on using precomputed data. Thus, there are a lot of auxiliary materials that come with a code. To date, we have lists of irreducible polynomials up to degree 6, a list of values of Gauss sums of the form $G(f, f^2)$, where f is square-free, for $\deg f \leq 3$, and a list of values of Gauss sums of the form $G(1, f)$ for f square-free up to degree 6.

7 Results

In this section, we present and discuss in more detail the computations and the data we obtained. Overall, we have computed zeros of over 100,000 polynomials $P(V, i, u^3)$, and covered all linear cases and some quadratic. We will assume $q = 7$ from now on.

To start with, we recall that the degree of the polynomial $P(V, i, u^3)$ is at most $[(1 + \deg V - i)/3]$. We want to emphasize that whenever we talk about the degree of $P(V, i, u^3)$, we always mean the degree in $x = u^3$, where $u = q^{-s}$. Thus, even in the "linear" case, we have, in fact, a cubic polynomial in u, with each of the three roots being a conjugate of one another.

On all the graphs, except for those where it is specified otherwise, we will plot the roots of $P(V, i, u^3)$ up to conjugate by plotting only one of the solutions to $u^3 = x$ for $P(V, i, x) = 0$. When the roots accumulate around a certain point (i.e. Figures 3, 5, 8, etc.), we will plot the entire cluster. If they are spread around the plane (i.e. Figure 4, 9, etc.), we will only plot the roots with the arguments falling in the interval $[-\pi/3, \pi/3]$. Also, we will plot circles of various radii as reference scale. Notice that the critical strip for $\psi(V, i, u)$ is between the circles $|u| = q^{-2}$ and $|u| = q^0 = 1$. Starting at $\deg P(V, i, u^3) = 2$, we will consider square-free and non-square-free polynomials separately, since, by Proposition 5.4, non-square-free polynomials will have at least one trivial zero.

In the table below we can see the degree of the polynomial P obtained from certain combinations of V of low degree and i.

i \ deg V	1	2	3	4	5	6	7	8	9
0	0	-	1	1	2	2	2	3	3
1	0	0	1	-	1	2	2	2	3
2	0	0	0	1	1	-	2	2	2

Table 1: The intersection of $\deg V$ and i is the degree of the polynomial $P(V, i, u^3)$, and - means $\rho(V, i) = 0$.

We proceed by taking a closer look at polynomials. For example, take an appropriate, i.e. square-free, V of degree 4 in $\mathbb{F}_q[t]$ and let $i = 2$. Then, by Proposition 5.4,

$\deg P(V,2,u^3) = 1$ and the polynomial is given as

$$P(V,2,u^3) = C(V,2) + \big(C(V,2)(q^3 - q^4) + C(V,5)\big)u^3.$$

Our approach to generating a single dataset was as follows: we fix a degree of a conductor V and a parameter i such that

$$i - 2\deg V \equiv 0 \text{ or } 1 \mod 3,$$

so that we obtain a non-trivial zero, i.e. $P(V,i,q^{-4}) \neq 0$. For a fixed degree of a conductor we always have only two options for the value of i that would result in $\rho(V,i) \neq o$, and therefore two datasets. For each such case we will present the data separately.

Although the roots appear increasingly random as the degree of $P(V,i,u^3)$ increases, there are still some conclusions we can draw from the data. First, as predicted, not all the roots are on the critical line $\Re(s) = 1$, thus confirming our initial hypothesis that the Riemann hypothesis is not satisfied for this series.

Another apparent pattern is the similarity between the roots derived from $\deg V = 3$ and $\deg V = 4$. We explain more of it in the following proposition.

Proposition 7.1. *Let $V \in \mathbb{F}_q[t]$ be a monic square-free polynomial of degree 3 or 4. Then the polynomial $P(V,0,u^3)$ be linear and it has 6 possible roots up to conjugate. Furthermore, if $V \in \mathbb{F}_q[t]$ is of degree 3, and we let $g(x) = V(x)\cdot(x-\alpha)$, then $P(V,0,u^3)$ has the same roots up to conjugation as $P(g,0,u^3)$.*

Proof. If $i = 0$ and $\deg P = 1$, we have

$$P(V,0,u^3) = 1 + u^3[(q^3 - q^4) + C(V,3)].$$

Using Proposition 5.4, as described in the last part of the previous section, and Theorem 4.3, we obtain the following.

$$\begin{aligned}(q^3 - q^4) + C(V,3) &= q^4(\rho(V,0) - 1)\\ &= q^4(\overline{G(1,V)}|V|^{-2/3} - 1)\\ &= q^4(\overline{\mu(V)\Big(\frac{V'}{V}\Big)_3(-\tau(\chi_3))^{\deg V}}|V|^{-2/3} - 1).\end{aligned} \tag{15}$$

Since there 2 possible values of $\mu(V)$ and 3 of $\left(\frac{V'}{V}\right)_3$, we conclude that there are only 6 possible values for the value of the expression above, and therefore only 6 possible polynomials.

Now, fix $\deg V = 3$. Then, by Proposition 5.4,

$$\rho(V,0) = \overline{G(1,V)}|V|^{-2/3}.$$

Let $g(x) = V(x)\cdot(x-\alpha)$, where $\alpha \in \mathbb{F}_q[x]$ and $((x-\alpha),V) = 1$. Before proceeding, notice that if $h(x) = x - \alpha$, where $\alpha \in \mathbb{F}_q[t]$, then

$$G(1,h) = \sum_{a\in\mathbb{F}_q^*}\Big(\frac{a}{h}\Big)_3 e\Big(\frac{a}{h}\Big) = \sum_{a\in\mathbb{F}_q^*} a^{\frac{q-1}{3}} e^{2\pi i a/3} = \tau(\chi_3).$$

Then

$$\begin{aligned}\rho(g,0) &= \overline{\left(\frac{h}{V}\right)_3 G(1,V)G(1,(h))}|g|^{-2/3}q^{4/3}\tau(\chi_3)q \\ &= \overline{\left(\frac{h}{V}\right)_3 G(1,V)}\tau(\chi_3)\tau(\chi_3)q^{-3} \\ &= \overline{\left(\frac{h}{V}\right)_3 G(1,V)}q^{-2} = \overline{\left(\frac{h}{V}\right)_3}\rho(V,0).\end{aligned}$$

Combining it with (12) completes the proof. □

Unfortunately, this approach is difficult to extend beyond the linear of $i = 0$, since their constant term is not necessarily equal to 1. If one manages to do that, this would imply that polynomials of conductors of higher degree can be obtained from those of lower degree corresponding to their divisors. Potentially, it could limit the inputs to just irreducible polynomials. From the computation point of view, it will be highly beneficial, as it would allow to only use Theorem 4.3 during computations.

We can also see that some roots accumulate around the pole at $q^{-4/3}$. In the linear cases we can still see some oscillation. For example, when $\deg V = 3$, they are "centered" around the point for $i = 0$ and are "distanced" for $i = 1$. This becomes less apparent in the quadratic case, but nevertheless still holds. Despite now having two roots, one of the two roots of each polynomial always stays close to $q^{-4/3.}$ For example, for $\deg V = 6$ and $i = 0$ we again can see the roots tightly packed around $q^{-4/3}$. Whereas for $i = 1$, they still form a circle around the point, but it is not as dense.

The oscillations away from and towards $q^{-4/3}$ seem to be correlated with the value of the polynomial at that point. Take $\deg V = 4$. Since in this case the function is linear, it cannot swing away and a small absolute value of the polynomial at the point indicates the proximity to the zero. By Proposition 5.4, we have $|\rho(V,0)| = q^{-1/2}$ and $|\rho(V,2)| = q^2$. In the first case the absolute value is relatively small and, indeed, we see all the roots centered closely around $q^{-4/3}$. On the contrary, when $i = 2$, we have the size of the polynomial evaluated at $q^{-4/3}$ being quite big and all the roots are away from the point.

We hypothesize that as the degree of $P(V, i, u^3)$ goes to infinity, one root of the polynomial tends to get closer to the point $u = q^{-4/3}$. If we look again at the residue as given in Proposition 5.4, we see that with the growth of degree of V it is quickly overwhelmed by

$$|G(1,V)| \cdot |V|^{-2/3} = |V|^{-1/6}.$$

Therefore, the absolute value of the residue decreases as the degree of the conductor increases. Hence, under such conditions, it is not unexpected to find a root around the pole.

8 Graphs

8.1 Linear

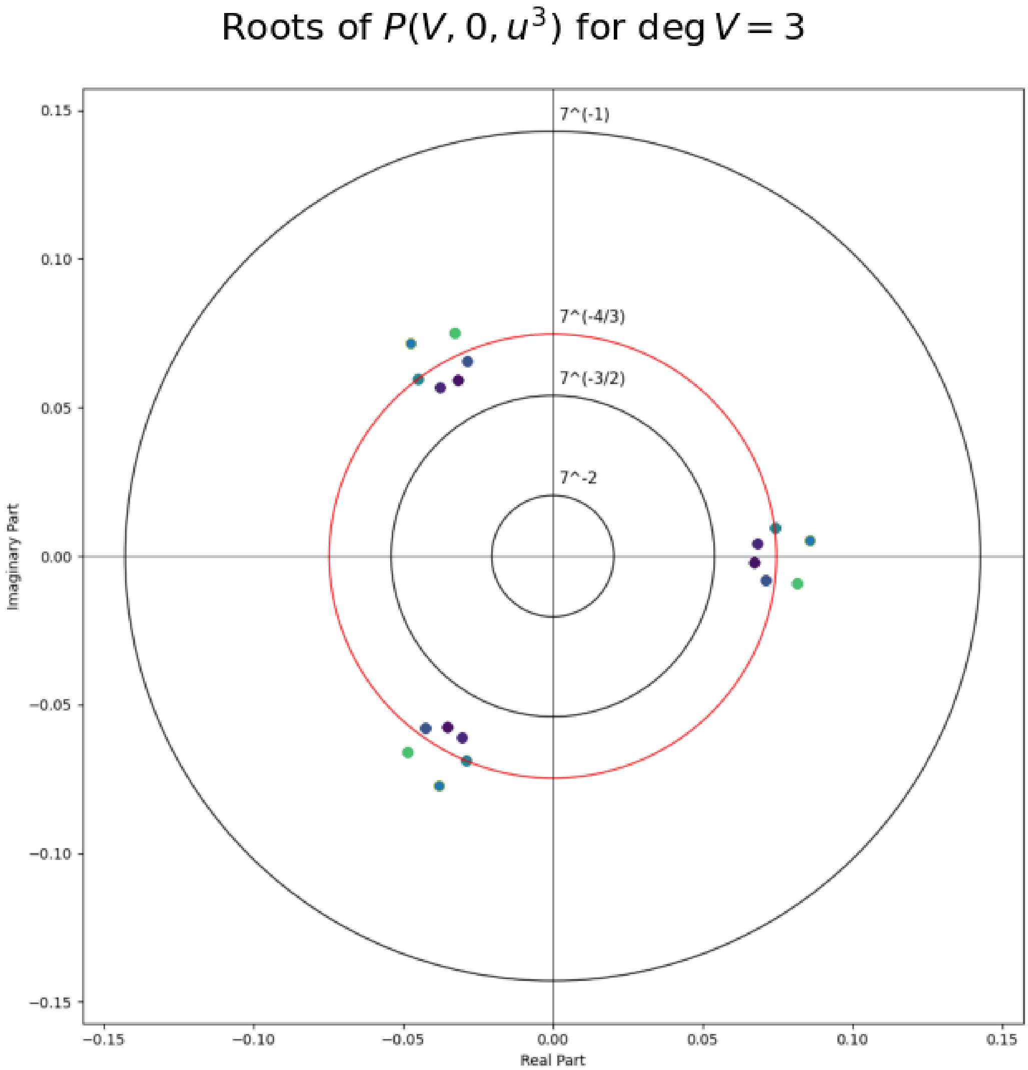

Figure 1: This graph shows the 3 conjugate roots of the linear polynomial $P(f, 0, u^3)$ as f varies over all monic square-free polynomials of degree 3 in $\mathbb{F}_7[x]$. There are $7^4 - 7^3 = 294$ such polynomials, but only 6 possible values for $P(f, 0, u^3)$, which follows from Proposition 5.4, as we explain in Section 7.

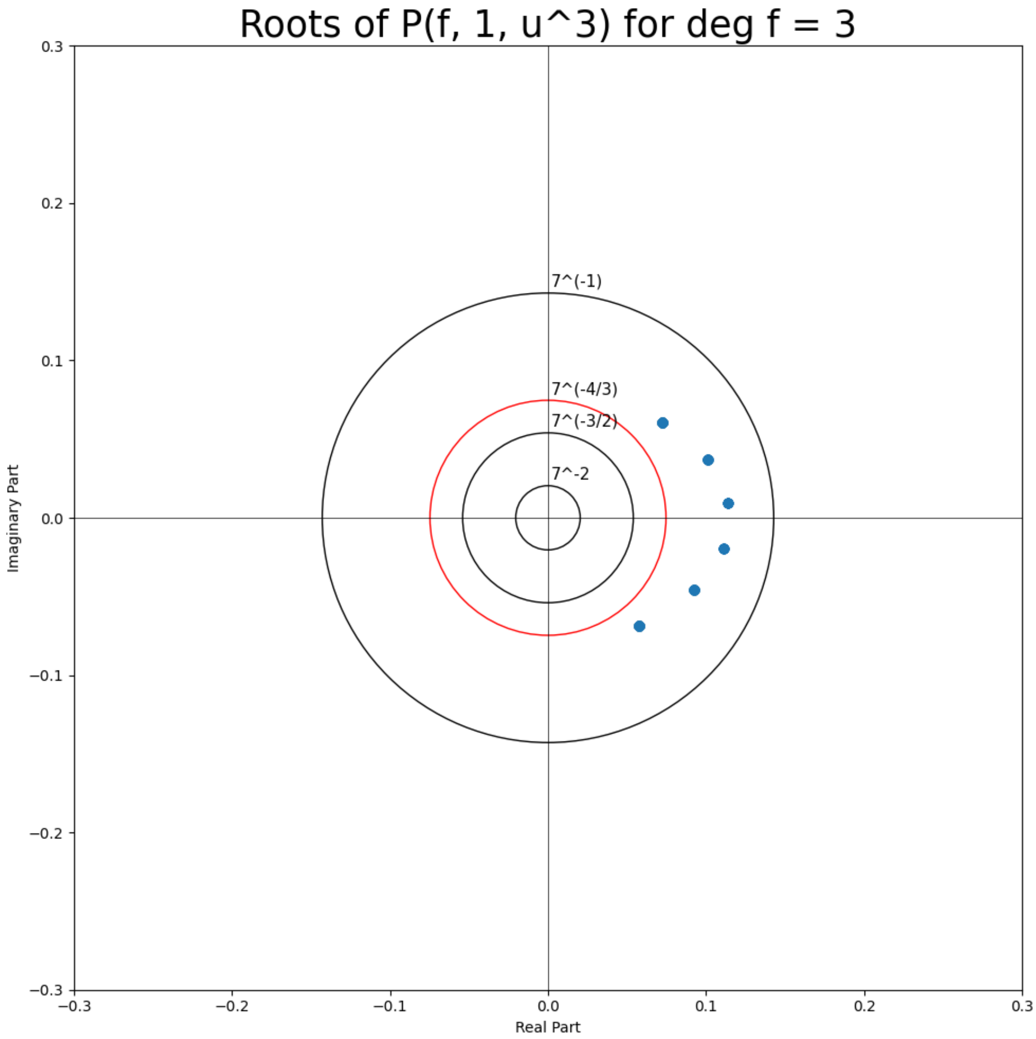

Figure 2: The graph shows one of three conjugate roots of a linear $P(f, 1, u^3)$ as f varies over all $7^3 - 7^2 = 294$ monic square-free polynomials of degree 3 over $\mathbb{F}_7$.

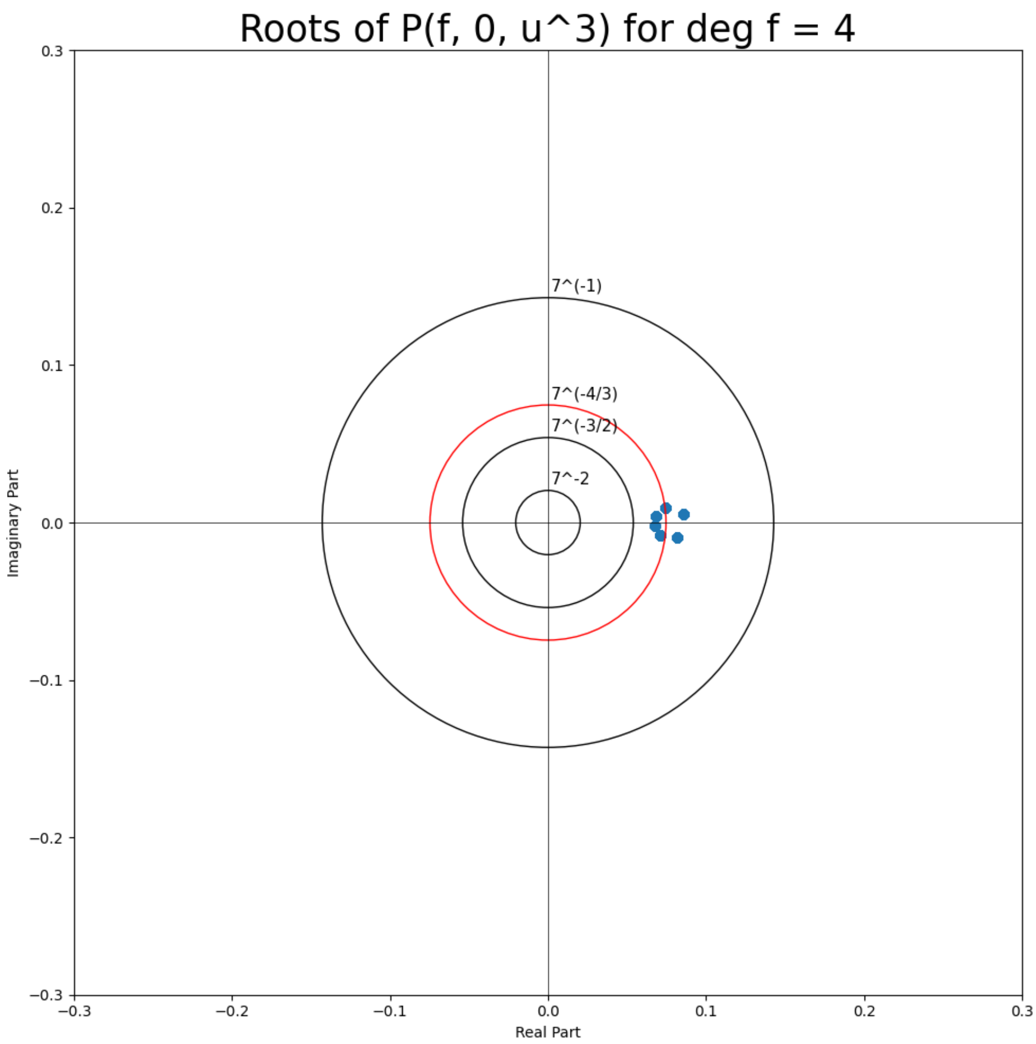

Figure 3: The graph shows one of three conjugate roots of a linear $P(f, 0, u^3)$ as f varies over all $7^4 - 7^3 = 2058$ monic square-free polynomials of degree 4 over $\mathbb{F}_7$.

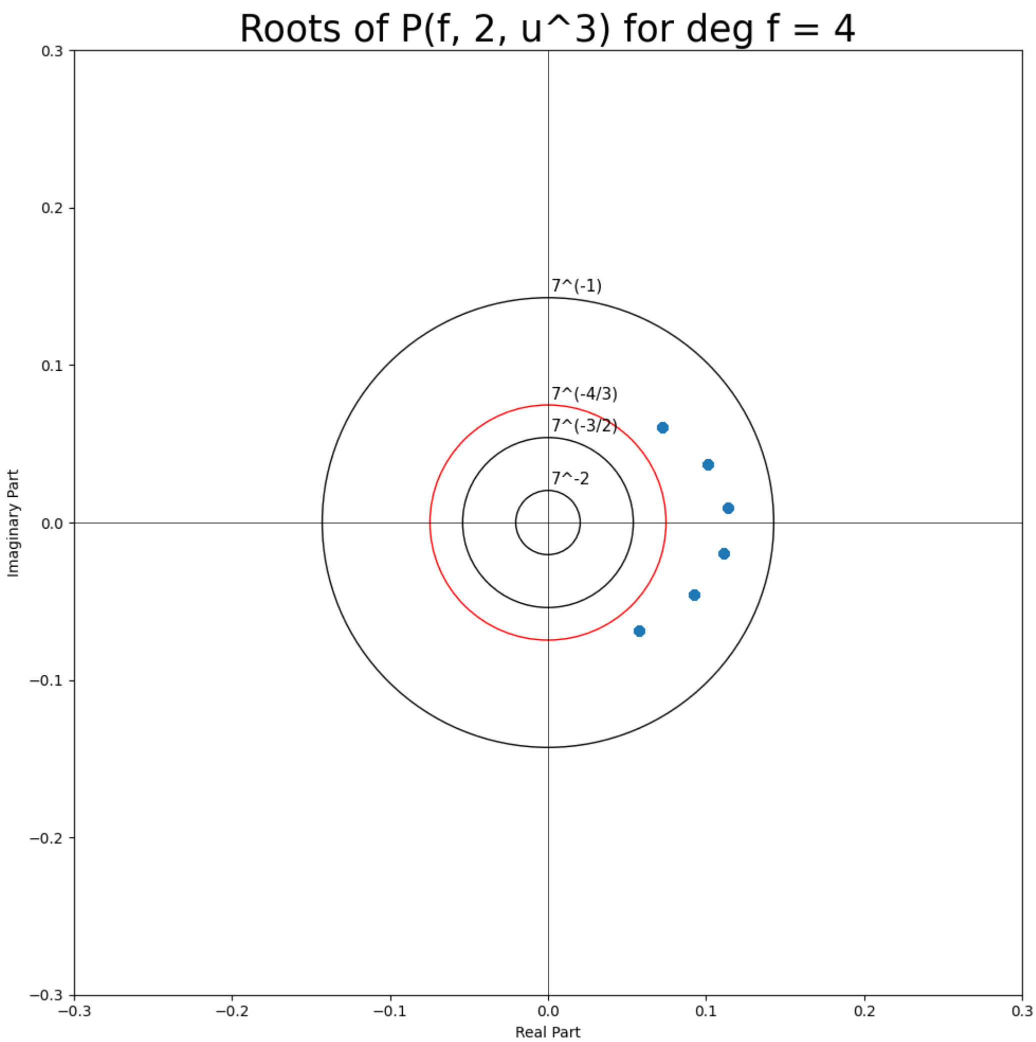

Figure 4: The graph shows one of three conjugate roots of a linear $P(f, 2, u^3)$ as f varies over all $7^4 - 7^3 = 2058$ monic square-free polynomials of degree 4 over $\mathbb{F}_7$.

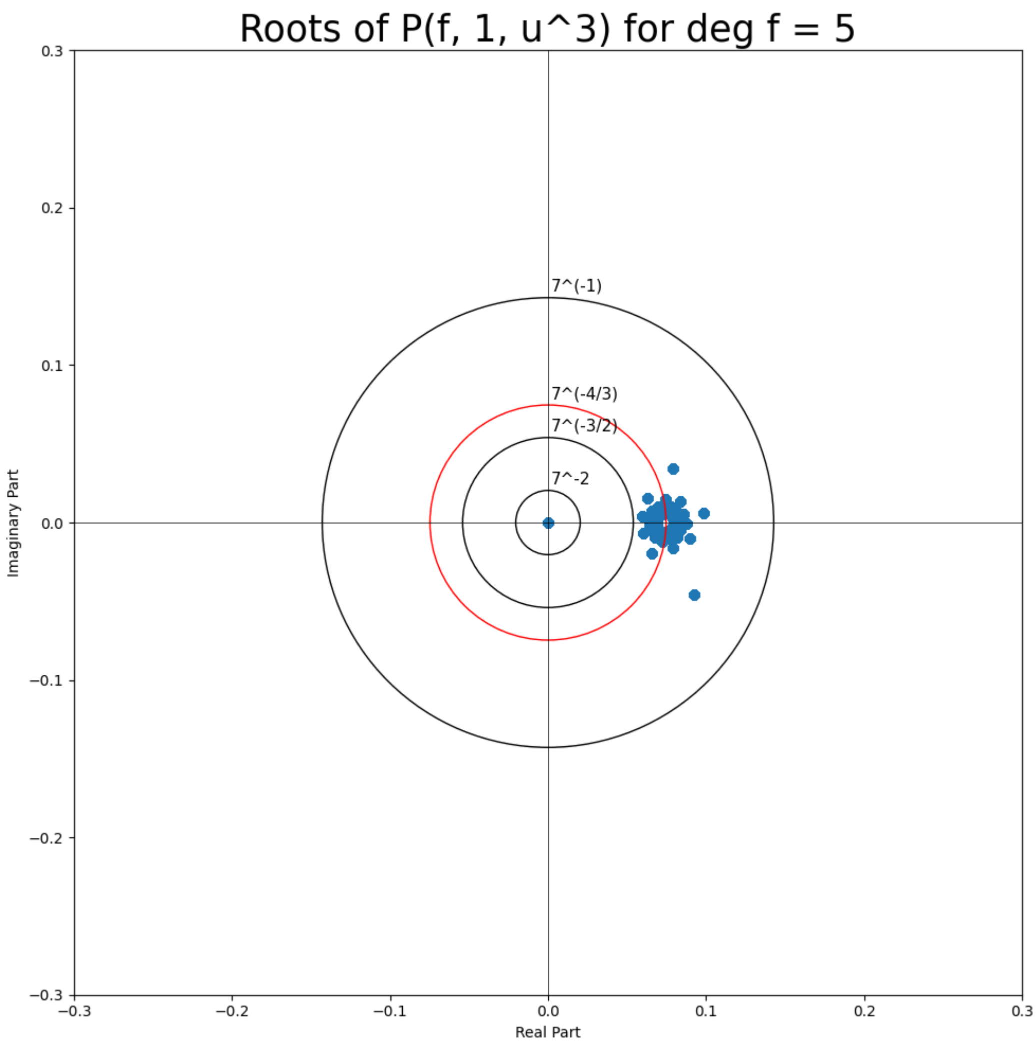

Figure 5: The graph shows one of three conjugate roots of a linear $P(f, 1, u^3)$ as f varies over all $7^5 - 7^4 = 14406$ monic square-free polynomials of degree 5 over $\mathbb{F}_7$. Notice that there some 763 polynomials with a root at the point $x = 0$, that would be the first root outside of the critical strip.

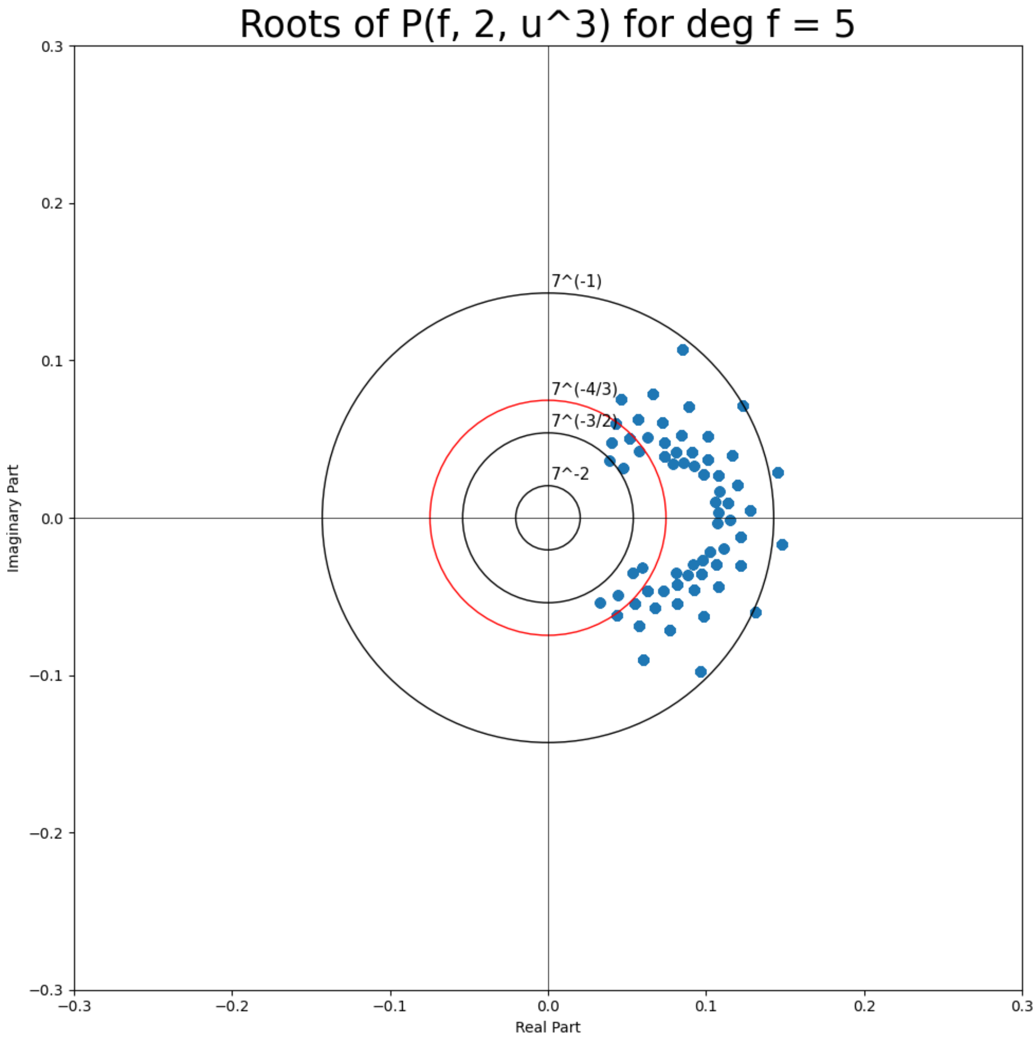

Figure 6: The graph shows one of three conjugate roots of a linear $P(f, 2, u^3)$ as f varies over a subset of 13608 monic square-free polynomials of degree 5 over $\mathbb{F}_7$. There are 798 polynomials V that result in a $P(f, 2, u^3)$ having degree 0, thus they are excluded.

8.2 Quadratic

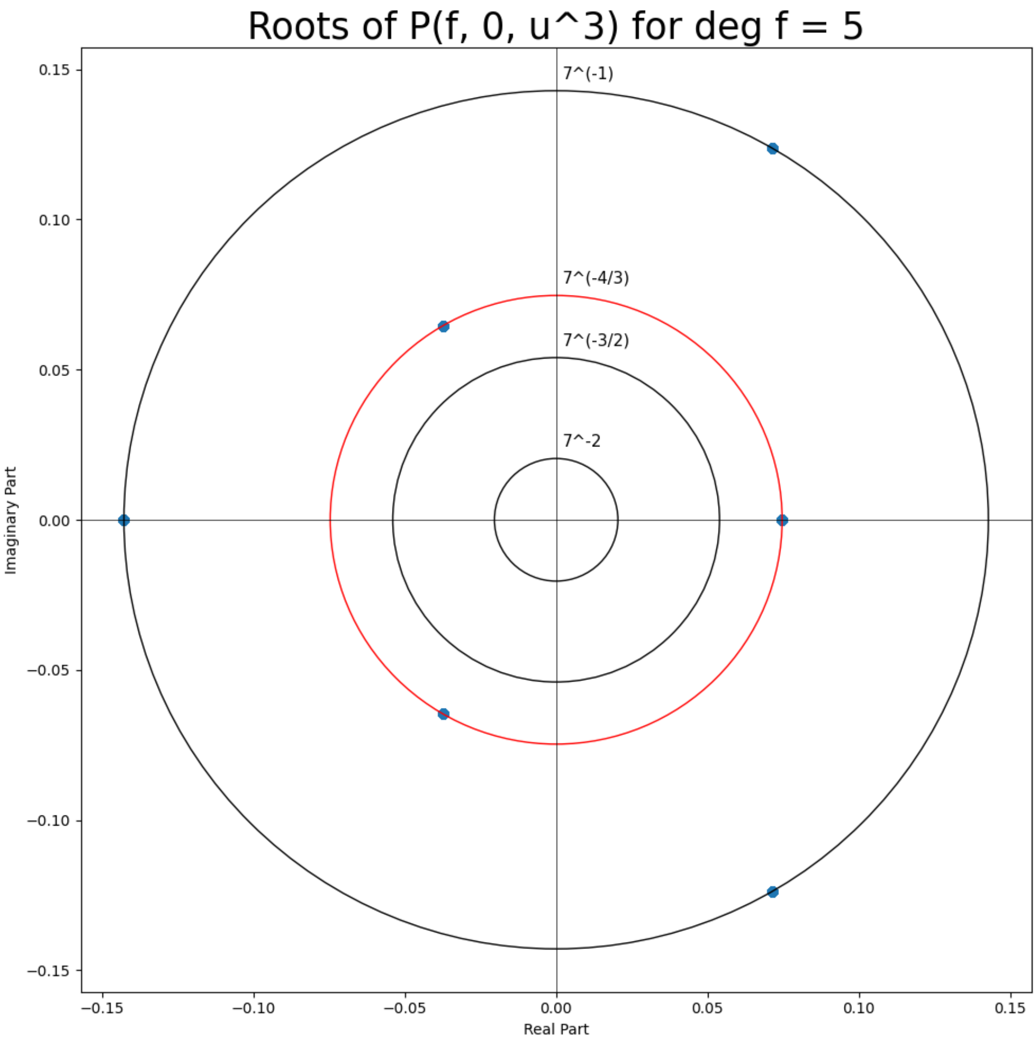

Figure 7: The graph shows all roots, including conjugates, of a quadratic $P(f, 0, u^3)$ as f varies over all $7^5 - 7^4 = 14406$ monic square-free polynomials of degree 5 over $\mathbb{F}_7$. Note that the roots are exactly at points $x = 7^{-1}$ and $x = 7^{-4/3}$. Non-square-free polynomials yield the exact same roots

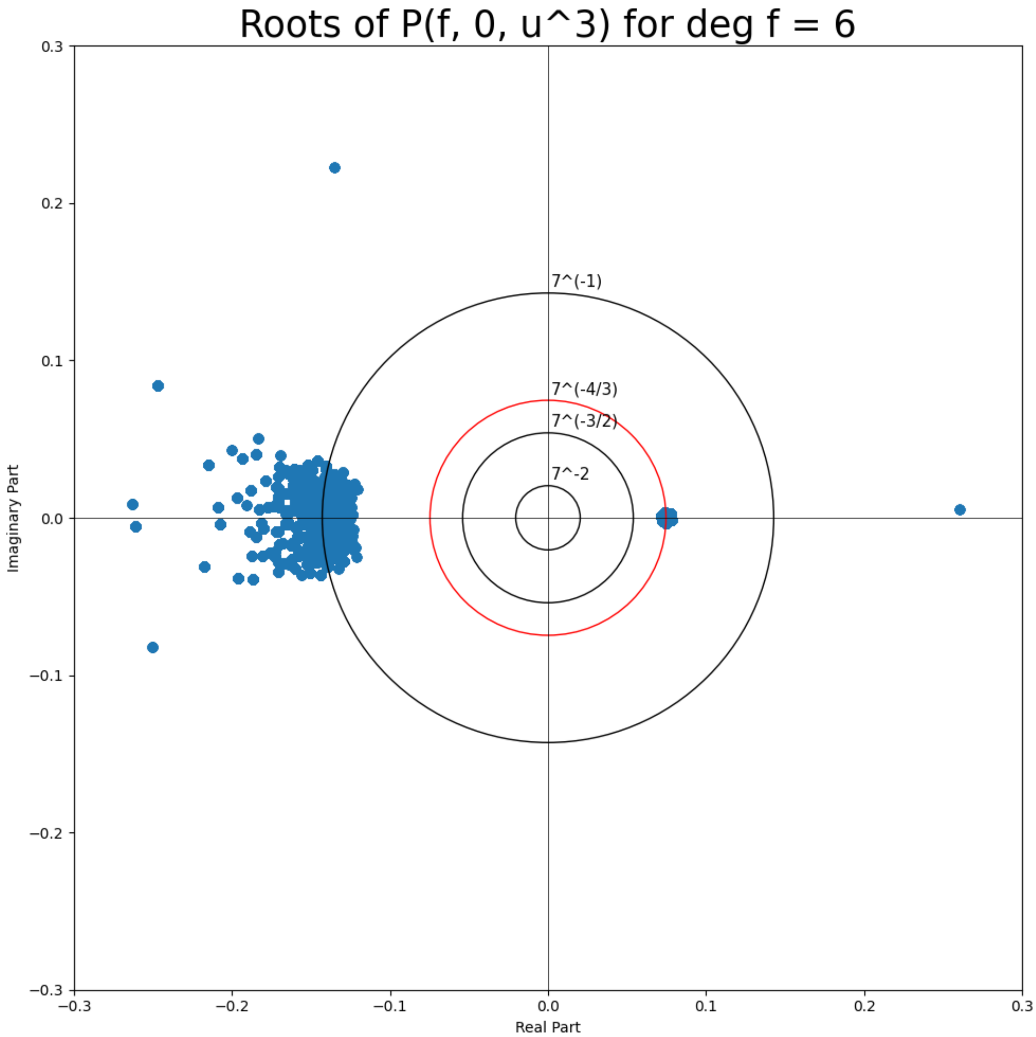

Figure 8: The graph shows roots up to a conjugate of a quadratic $P(f, 0, u^3)$ as f varies over of all 100842 monic square-free polynomials of degree 6 over $\mathbb{F}_7$. For all inputs, the polynomial always has one root near $7^{-4/3}$ and another falling in the second cluster.

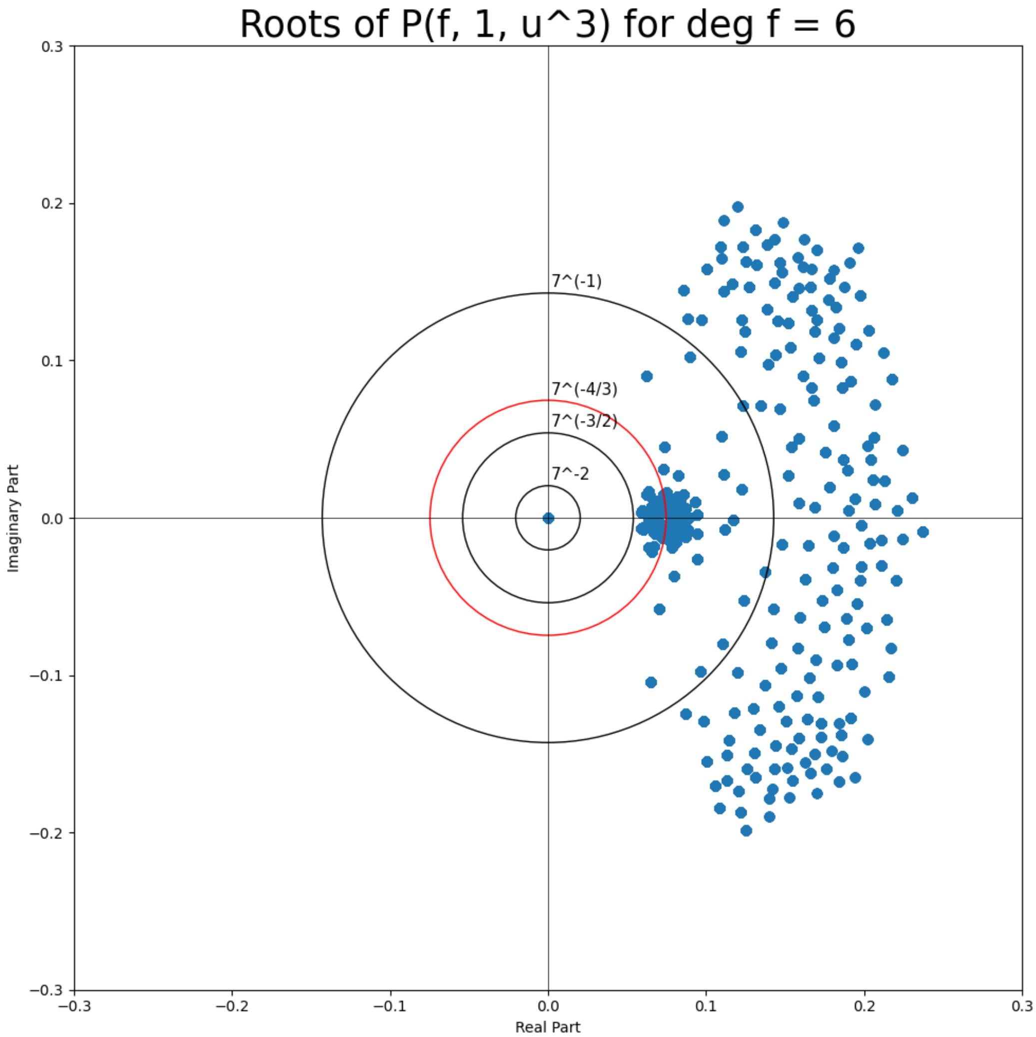

Figure 9: The graph shows roots up to a conjugate of a quadratic $P(f, 1, u^3)$ as f varies over a subset of monic square-free polynomials of degree 7 over $\mathbb{F}_7$. Not all the monic square-free polynomials were processed due to hardware limitations. $\deg P(f, 1, u^3) = 2$, both roots are at least at the distance 1e-5 from each other.

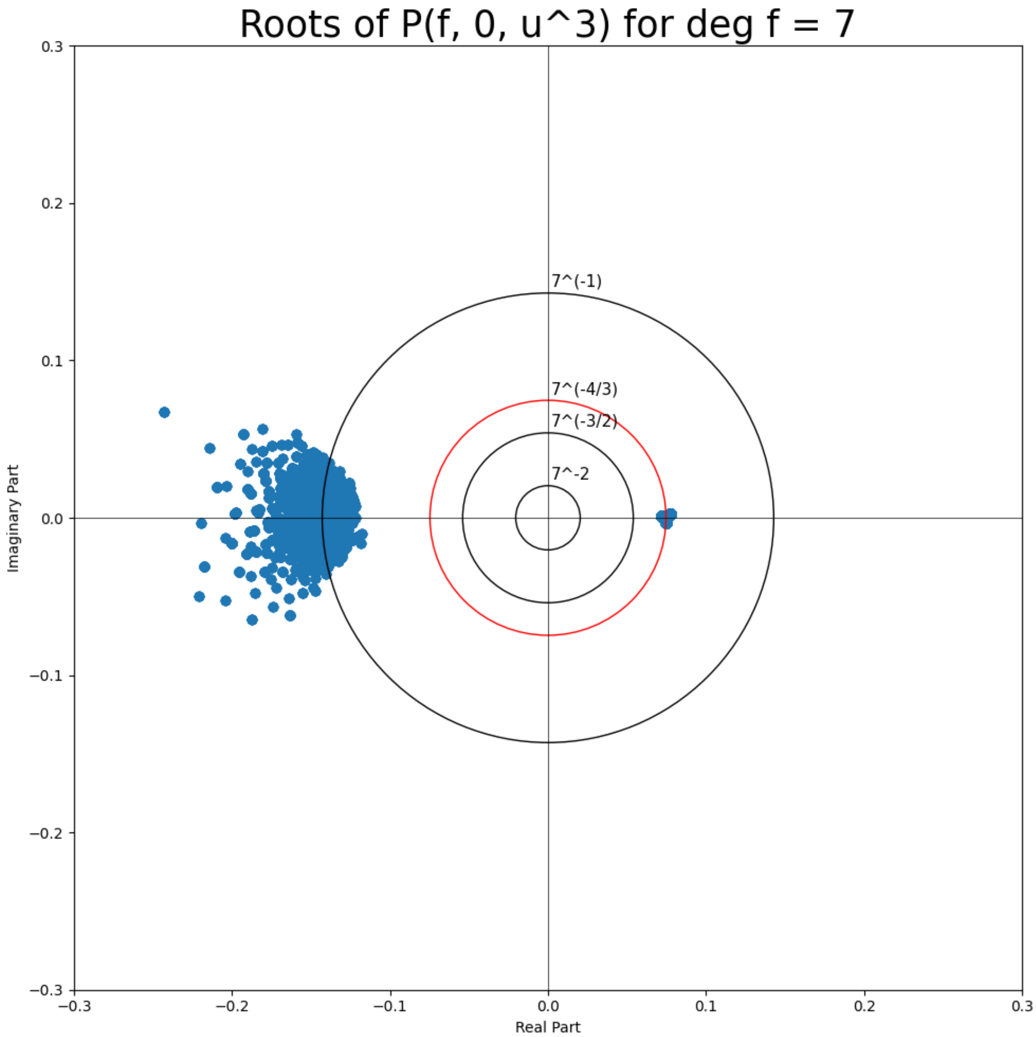

Figure 10: The graph shows roots up to a conjugate of a quadratic $P(f, 0, u^3)$ as f varies over a subset of irreducible polynomials of degree 7 over $\mathbb{F}_7$. Not all the monic square-free polynomials were processed due to hardware limitations. For all inputs, the polynomial always has one root near $7^{-4/3}$ and another falling in the second cluster.

9 References

References

[DFL22] Chantal David, Alexandra Florea, and Matilde Lalín. The mean values of cubic l-functions over function fields. *Algebra & Number Theory*, 16(5):1259–1326, 2022.

[Hof92] Jeffrey Hoffstein. Theta functions on the n-fold metaplectic cover of sl (2)—the function field case. *Inventiones mathematicae*, 107(1):61–86, 1992.

[IR90] Kenneth Ireland and Michael Ira Rosen. *A classical introduction to modern number theory*, volume 84. Springer Science & Business Media, 1990.

[KP84] David A Kazhdan and Samuel J Patterson. Metaplectic forms. *Publications Mathématiques de l'IHÉS*, 59:35–142, 1984.

[Kub69] Tomio Kubota. *On automorphic functions and the reciprocity law in a number field*, volume 2. Kinokuniya, 1969.

[Kub06] Tomio Kubota. Some number-theoretical results on real analytic automorphic forms. In *Several Complex Variables II Maryland 1970: Proceedings of the International Mathematical Conference, held at College Park, April 6–17, 1970*, pages 87–96. Springer, 2006.

[Pat78] SJ Patterson. On the distribution of kummer sums. 1978.

[Pat07] SJ Patterson. Note on a paper of j. hoffstein. *Glasgow Mathematical Journal*, 49(2):243–255, 2007.

[PHB79] SJ Patterson and DR Heath-Brown. The distribution of kummer sums at prime arguments. 1979.

[Ros13] Michael Rosen. *Number theory in function fields*, volume 210. Springer Science & Business Media, 2013.

[Sti09] Henning Stichtenoth. *Algebraic function fields and codes*. Springer, 2009.