Irreducible polynomials over $\mathbb{F}_{2^r}$ with three prescribed coefficients

Ofir Gorodetsky

Abstract

For any positive integers $n \geq 3$ and $r \geq 1$, we prove that the number of monic irreducible polynomials of degree $n$ over $\mathbb{F}_{2^r}$ in which the coefficients of $T^{n-1}$, $T^{n-2}$ and $T^{n-3}$ are prescribed has period 24 as a function of $n$, after a suitable normalization. A similar result holds over $\mathbb{F}_{3^r}$, with the period being 60. We also show that this is a phenomena unique to characteristics 2 and 5. The result is strongly related to the supersingularity of certain curves associated with cyclotomic function fields, and in particular it complements an equidistribution result of Katz.

1 Introduction

Let $q = p^r$ be a prime power and let $\mathbb{F}_q$ denote the finite field containing $q$ elements. Let $\mathbb{F}_q[T]$ denote the polynomial ring over $\mathbb{F}_q$ in indeterminate $T$. Let $\mathcal{M}_{n,q}$ denote the set of monic polynomials of degree $n$ in $\mathbb{F}_q[T]$ and $\mathcal{M}_q = \bigcup_{n \geq 0} \mathcal{M}_{n,q}$ denote the set of all monic polynomials in $\mathbb{F}_q[T]$. Let $\mathcal{P}_q$ denote the set of irreducible polynomials in $\mathcal{M}_q$. We adopt throughout the following conventions: The $j$-th next-to-leading coefficient of a polynomial $f(T) \in \mathcal{M}_q$ with $j > \deg f$ is considered to be 0. We assume that $0 \in \mathbb{N}$.

A classical result due to Gauss \cite{Gau65} pp. 608-611] is that the number $\pi_q(n)$ of polynomials of degree $n \geq 1$ in $\mathcal{P}_q$ is given by

$$\pi_q(n) = \frac{1}{n} \sum_{d|n} \mu(d) q^{n/d}, \quad (1.1)$$

where $\mu$ is the usual Möbius function. A natural extension of this problem is to determine the number of monic irreducible polynomials in $\mathbb{F}_q[T]$ of degree $n$ for which the first $\ell$ next-to-leading coefficients have the prescribed values $t_1, \ldots, t_{\ell}$, while the remaining coefficients are arbitrary. Formally, if we let $1_{\mathcal{P}_q} : \mathcal{M}_q \to \mathbb{C}$ be the indicator of primes in $\mathcal{M}_q$, then one may study the function

$$\pi_q(n, t_1, \ldots, t_{\ell}) = \sum_{f \in \mathcal{M}_{n,q}, \text{first } \ell \text{ next-to-leading coefficients of } f \text{ are } t_1, \ldots, t_{\ell}} 1_{\mathcal{P}_q}(f).$$

We note that $\pi_q(n, t_1, \ldots, t_{\ell})$ makes sense for any $\ell \in \mathbb{N}$, including $\ell = 0$ and $\ell > n$. Part of the motivation for studying $\pi_q(n, t_1, \ldots, t_{\ell})$ is the following observation. If we let $f(T) = T^n + t_1 T^{n-1} + \ldots + t_{\ell} T^{n-\ell}$,

then $\pi_q(n, t_1, \ldots, t_{\ell})$ counts the number of irreducible polynomials in the set

$$\{ g \in \mathbb{F}_q[T] : \deg(g - f) < n - \ell \},$$

which is a polynomial analogue of an interval in $\mathbb{Z}$, see the discussion in Keating and Rudnick \cite{KR14} Sec. 2.1. The problem of counting integer primes in an interval has a long history. If we let $\pi(x) = \# \{0 < p \leq x : p \text{ is a prime} \}$ be the prime counting function, then the prime number theorem states that

$$\pi(x) \sim \frac{x}{\ln x}, \quad x \to \infty.$$  

Therefore, one may expect that if $\Phi(x)$ is a function that tends to infinity slower than $x$ but not too slow, then the ‘short’ interval $[x, x + \Phi(x)]$ contains about $\frac{\Phi(x)}{\ln x}$ primes, that is,

$$\pi(x + \Phi(x)) - \pi(x) \sim \frac{\Phi(x)}{\ln x}, \quad x \to \infty. \quad (1.2)$$

1
It is conjectured \cite[7]{Gra95} that \eqref{estimates} holds for \( \Phi(x) = x^\varepsilon \) for any \( \varepsilon \in (0, 1) \). Von Koch \cite{vK01} showed that the Riemann Hypothesis implies that \eqref{estimates} holds for \( \Phi(x) = \sqrt{x} \ln^2 x \). Heath-Brown \cite{HB88}, improving on Huxley \cite{Hux74}, proved that \eqref{estimates} holds unconditionally for \( \Phi(x) = x^{1/3-\varepsilon(x)} \), where \( \varepsilon(x) \to 0 \) as \( x \to \infty \).

For \( \ell < \frac{1}{2} \), methods similar to the ones in the integer setting yield good estimates for \( \pi_q(n, t_1, \ldots, t_\ell) \). In the polynomial setting the Riemann Hypothesis for \( L \)-Functions was established by Weil \cite{Wei74}, from which one can deduce

\[
\pi_q(n, t_1, \ldots, t_\ell) = q^{n-\ell} n + O \left( \frac{\ell + 1}{n} q^{\frac{n}{2}} \right),
\]

\eqref{estimate}. see Rhin \cite[Thm. 4]{Rhi72} (cf. Hsu \cite[Cor. 2.6]{Hsu96}). For \( n - 4 \geq \ell \geq \frac{q}{2} \), asymptotic results are known only in the limit \( q \to \infty \), and the methods come from Galois theory. These methods give

\[
\pi_q(n, t_1, \ldots, t_\ell) = q^{n-\ell} n + O \left( q^{\alpha - \ell - \frac{1}{2}} \right),
\]

\eqref{estimate2}. see the works of Cohen \cite[Thm. 1]{Col72} and Bank, Bary-Soroker and Rosenzweig \cite[Thm. 2.3]{BBR03}.

Apart from asymptotic results, several exact results are known. Carlitz obtained formulas for \( \pi_q(n, t_1) \) in 1952 \cite[Thm. 3]{Car52}, and Kuz'min obtained formulas for \( \pi_q(n, t_1, t_2) \) in 1991 \cite[Thms. 1-4]{Kuz91}.

Both Carlitz and Kuz'min have used extensively in their proofs \( L \)-functions of certain characters. Later, several authors have reproved the results of Carlitz and Kuz'min without employing \( L \)-functions. Ruskey et al. \cite[Thm. 1.1]{RMS01} and Yucas \cite[Cor. 2.7]{Yuc06} reproduced Carlitz' result. Cattell et al. reproduced Kuz'min’s result for the case \( q = 2 \) \cite[Thms. 1-4]{CMR03}, and Ri et al. reproduced Kuz'min’s result for the case that \( q \) is a power of 2 \cite[Thms. 1-4]{RMKR14}. Recently, Lalín and Larocque \cite{LL16} obtained a combinatorial proof of Kuz'min's result.

Apart from Carlitz’s and Kuz'min’s work on \( \pi_q(n, t_1, t_2) \), some other interesting exact results are known. Kuz'min determined \( \pi_q(4, t_1, t_2, t_3) \) for any \( q \) \cite{Kuz94}. Yucas and Mullen computed \( \pi_2(n, t_1, t_2, t_3) \) for \( n \) even \cite[Thm. 4]{YAM04} and FitzGerald and Yucas computed \( \pi_2(n, t_1, t_2, t_3) \) for odd \( n \) \cite[Thm. 3.4]{FY03}. Molitsio and Ranto \cite[Lem. 19]{MR08} computed \( \sum_{t_2 \in \mathbb{F}_q} \pi_q(n, 0, t_2, t_3) \) for any given \( t_3 \in \mathbb{F}_q \). Recently, Ahmad et al. computed \( \pi_2(n, 0, 0, 0) \) for any \( n \) \cite[Thm. 8]{AGG+16}. The mentioned papers again did not employ \( L \)-functions.

### 1.1 Counting with von Mangoldt

Let \( \Lambda_q : \mathcal{M}_q \to \mathbb{C} \) be the von Mangoldt function, defined as

\[
\Lambda_q(f) = \begin{cases} 
\deg P & \text{if } f = P^k, \text{ } P \text{ irreducible}, \\
0 & \text{otherwise},
\end{cases}
\]

\eqref{von-Mangoldt-definition}. The von Mangoldt function counts prime powers with weights, and is closely related to the indicator of primes, \( 1_{P_q} \). Let \( \psi_q : \mathbb{N} \to \mathbb{C} \) be the summatory function of \( \Lambda_q \):

\[
\psi_q(n) = \sum_{f \in \mathcal{M}_{n,q}} \Lambda_q(f).
\]

\eqref{von-Mangoldt-summatory}. We have the following classical result for any positive integer \( n \), from which \eqref{von-Mangoldt-summatory} is usually derived \cite[Prop. 2.1]{Ros02}:

\[
\psi_q(n) = q^n.
\]

\eqref{von-Mangoldt-classical}. Given \( t_1, \ldots, t_\ell \in \mathbb{F}_q \), we denote by \( \psi_q(n, t_1, \ldots, t_\ell) \) the sum of \( \Lambda_q \) over elements of \( \mathcal{M}_{n,q} \) whose first \( \ell \) next-to-leading coefficients are \( t_1, \ldots, t_\ell \):

\[
\psi_q(n, t_1, \ldots, t_\ell) = \sum_{f \in \mathcal{M}_{n,q}, \text{ first } \ell \text{ next-to-leading coefficients of } f \text{ are } t_1, \ldots, t_\ell} \Lambda_q(f).
\]

\eqref{von-Mangoldt-multiple}. A standard Möbius inversion argument allows one to switch between \( \psi_q(n, \bullet, \ldots, \bullet) \) and \( \pi_q(n, \bullet, \ldots, \bullet) \). This is done explicitly in Proposition \ref{von-Mangoldt-prop} for any \( \ell \) and in Corollary \ref{von-Mangoldt-cor} for \( \ell = 3 \). The estimate \eqref{von-Mangoldt-estimate} takes the following form in the language of \( \psi_q \):

\[
\psi_q(n, t_1, \ldots, t_\ell) = q^{n-\ell} + O \left( (\ell + 1)q^{\frac{n}{2}} \right).
\]

\eqref{von-Mangoldt-estimate2}.
1.2 Results

In [AGG+16 Thm. 8], the value of the function $\psi_q(n,0,0,0)$ was determined for any $q$ which is a power of 2. Let

$$f_q(n,t_1,t_2,t_3) = \frac{\psi_q(n,t_1,t_2,t_3) - q^{n-3}}{q^{n/2}}.$$

The authors of [AGG+16] proved that $f_q(n,0,0,0)$ has period 24 in $n$ starting from $n = 3$, that is,

$$f_{2^r}(n + 24, 0, 0, 0) = f_{2^r}(n, 0, 0, 0)$$

for all $r \geq 1$ and $n \geq 3$. Ahmadi et al. write [AGG+16 Sec. 9]: “Based on the $\mathbb{F}_2$ base field case and our result for $f_q(n,0,0,0)$, we conjecture that for $q = 2^r$, $n \geq 3$ and $t_1,t_2,t_3 \in \mathbb{F}_q$, the formulas for $f_q(n,t_1,t_2,t_3)$ all have period 24”. We prove this conjecture and exhibit some additional symmetries.

**Theorem 1.1.** Let $q = 2^r$. Let $t_1,t_2,t_3 \in \mathbb{F}_q$. Then

$$f_q(n,t_1,t_2,t_3) = \frac{\psi_q(n,t_1,t_2,t_3) - q^{n-3}}{q^{n/2}}$$

is periodic in $n \in \mathbb{N}_{>0}$ with period 24.

Additionally, the following symmetries hold. Let $n \geq 1$. If $\lambda \in \mathbb{N}_{>0}$ is coprime to 6, then

$$f_q(n,t_1,t_2,t_3) = f_q(\lambda n,t_1,t_2 + \left(\frac{\lambda}{2}\right) t_1^2,t_3 + \left(\frac{\lambda}{3}\right) t_1^3),$$

and if $d \in \mathbb{Z}$ is coprime to 6 and satisfies $d \equiv (\frac{n}{n,24})^{-1} \mod 24$, then

$$f_q(n,t_1,t_2,t_3) = f_q(n,24,t_1,t_2 + \left(\frac{d}{2}\right) t_1^2,t_3 + \left(\frac{d}{3}\right) t_1^3).$$

We prove an analogue of Theorem 1.1 for characteristic 5.

**Theorem 1.2.** Let $q = 5^r$. Let $t_1,t_2,t_3 \in \mathbb{F}_q$. Then

$$f_q(n,t_1,t_2,t_3) = \frac{\psi_q(n,t_1,t_2,t_3) - q^{n-3}}{q^{n/2}}$$

is periodic in $n \in \mathbb{N}_{>0}$ with period 60. (1.6)

Additionally, the following symmetries hold. Let $n \geq 1$. If $\lambda \in \mathbb{N}_{>0}$ is coprime to 30, then

$$f_q(n,t_1,t_2,t_3) = f_q(\lambda n,\lambda t_1,\lambda t_2 + \left(\frac{\lambda}{2}\right) t_1^2,\lambda t_3 + \lambda(\lambda-1)t_1t_2 + \left(\frac{\lambda}{3}\right) t_1^3),$$

and if $d \in \mathbb{Z}$ is coprime to 30 and satisfies $d \equiv (\frac{n}{n,60})^{-1} \mod 60$, then

$$f_q(n,t_1,t_2,t_3) = f_q(n,60,dt_1,dt_2 + \left(\frac{d}{2}\right) t_1^2,dt_3 + d(d-1)t_1t_2 + \left(\frac{d}{3}\right) t_1^3).$$

We prove a partial converse for Theorem 1.1 and Theorem 1.2.

**Theorem 1.3.** Let $\ell$ be a positive integer. Let $q = p^r$ be a prime power. Define the following function in variable $n \in \mathbb{N}_{>0}$:

$$f_{q,\ell}(n) = \frac{\psi_q(n,0,\ldots,0) - q^{n-\ell}}{q^{n/2}}.$$

If $\ell = 3$ and $p \notin \{2,5\}$ or $\ell \geq 4$, then the function $f_{q,\ell}(n)$ is not periodic in $n$.

From Theorems 1.1, 1.3 and Proposition 3.2 we immediately obtain the following result.

**Corollary 1.4.** Let $\ell$ be a positive integer and $q = p^r$ be a prime power. The function $f_{q,\ell}(n)$ defined in (1.9) is periodic in $n$ if and only if one of the following conditions hold.

1. $\ell = 1$, in which case the period is 1.
2. $\ell = 2$, in which case the period divides 4p.
3. \( \ell = 3, \ p \in \{2, 5\} \), in which case the period divides 12p.

We note that by (\ref{1.5}), it make sense to consider the periodicity of the normalized functions \( f_q(n, t_1, t_2, t_3) \) and \( f_{a, t}(n) \), as they are bounded as functions of \( n \).

We discuss an important consequence of Theorem \ref{1.1} namely, that it allows us to obtain formulas for \( \psi_2(n, t_1, t_2, t_3) \) for most values of \( n \). The last part of Theorem \ref{1.1} reduces the computation of \( \psi_2(n, t_1, t_2, t_3) \) to the computation of \( \psi_2((n, 24), t_1, t_2, t_3) \) for some \( t_i \). There are 8 possible values of \( (n, 24) \): 1, 2, 3, 4, 6, 8, 12 and 24. If \( (n, 24) = 1 \), then the computation of \( \psi_2((n, 24), t_1, t_2, t_3) \) is easy. Indeed,

\[
\psi_2(1, t_1, t_2, t_3) = 1_{t_2 + t_3 = 0},
\]

since there is no monic linear polynomial with first 3 next-to-leading coefficients equal to \( \tilde{t}_i \), unless \( t_2 = t_3 = 0 \), in which case there is one such polynomial: \( T + t_1 \). The case \( (n, 24) = 2 \) is similar – \( \psi_q(2, t_1, t_2, t_3) \) is 0 if \( \tilde{t}_3 \neq 0 \), and we obtain

\[
\psi_2(2, t_1, t_2, t_3) = \Lambda_2(T^2 + t_1T + t_2) \cdot 1_{t_2 = 0}.
\]

The case \( (n, 24) = 3 \) is also simple. The only monic cubic polynomial with 3 next-to-leading coefficients equal to \( \tilde{t}_i \) is \( T^3 + \tilde{t}_1T^2 + \tilde{t}_2T + \tilde{t}_3 \), and so

\[
\psi_2(3, t_1, t_2, t_3) = \Lambda_2(T^3 + \tilde{t}_1T^2 + \tilde{t}_2T + \tilde{t}_3),
\]

which may be computed using the irreducibility criteria for cubic polynomials in characteristic 2 [W175].

If \( (n, 24) = 4 \), the evaluation of \( \psi_q(4, t_1, t_2, t_3) \) was done by Kuz’min [Kuz94], and sometimes involves Kloosterman sums (depending on \( t_i \)). If \( (n, 24) = 24 \), then we have the following corollary of Theorem \ref{1.1} and its proof, proved in [3.5]

Corollary 1.5. Let \( q = 2^r \). Let \( t_1, t_2, t_3 \in \mathbb{F}_q \). Then

\[
\psi_q(24, t_1, t_2, t_3) = q^{21} - q^{10}(2q^2 \cdot 1_{t_1 = t_2 = t_3 = 0} - q \cdot 1_{t_1 = t_2 = 0} - 1_{t_1 = 0}).
\]

The cases \( (n, 24) \in \{6, 8, 12\} \) seem harder and we do not treat them here. In characteristic 5, Theorem \ref{1.2} similarly reduces the computation of \( \psi_5(n, t_1, t_2, t_3) \) to the computation of \( \psi_5((n, 60), t_1, t_2, t_3) \) for some \( \tilde{t}_i \). The cases \( (n, 60) \in \{1, 2, 3\} \) are again easy, \( (n, 60) = 4 \) was done by Kuz’min and \( (n, 60) = 60 \) treated in the following corollary, proved in [3.5]

Corollary 1.6. Let \( q = 5^r \). Let \( t_1, t_2, t_3 \in \mathbb{F}_q \). Then

\[
\psi_q(60, t_1, t_2, t_3) = q^{57} - q^{28}(2q^2 \cdot 1_{t_1 = t_2 = t_3 = 0} - q \cdot 1_{t_1 = t_2 = 0} - 1_{t_1 = 0}).
\]

1.3 Methods and interpretation

As in the works of Carlitz and Kuz’min, we use Dirichlet characters and \( L \)-Functions. This approach dates back to Dirichlet’s work on primes in arithmetic progressions. The Dirichlet characters that we use are defined modulo a power of the prime at infinity in \( \mathbb{F}_q(T) \). Concretely, we consider the group \( G(R_{3,q}) \) of characters whose value on \( f \in \mathcal{M}_q \) depends only the first \( \ell \) next-to-leading coefficients of \( f \), see \ref{2} for a precise definition. Lemma \ref{2.2} expresses \( f_q(n, t_1, t_2, t_3) \) as an average over \( G(R_{3,q}) \).

The main new ingredients in the proofs of Theorems \ref{1.1} and \ref{1.2} are Lemmas \ref{4} and \ref{4} respectively, which say the following. The roots of the \( L \)-function \( L(u, \chi) \) of a non-trivial character in \( G(R_{3,q}) \) are of the form \( \frac{\omega}{q^{3/2}} \), where \( \omega \) is a root of unity of order dividing 24 if \( q = 2 \), and dividing 60 if \( q = 5 \).

We now explain how Lemma \ref{5.5} relates to a result of Katz, and complements it. Fix a prime \( p \). For any non-trivial \( \chi \in G(R_{3,p^r}) \setminus G(R_{2,p^r}) \), we can write \( L(u, \chi) \) as

\[
L(u, \chi) = \det(I_2 - u\sqrt{p^r}\Theta_\chi),
\]

where \( \Theta_\chi \in U(2) \) is a unitary matrix, or rather a conjugacy class of such a matrix. Katz [Kat13] considered the distribution of the matrices \( \{\Theta_\chi\}_{\chi \in G(R_{3,p^r}) \setminus G(R_{2,p^r})} \) in \( PU(2) = U(2)/Z(U(2)) \) as \( r \to \infty \), in the following sense. He showed that if \( p \neq 2, 5 \), then for any continuous function \( f : U(2) \to \mathbb{C} \), invariant under conjugation and multiplication by scalars, we have

\[
\lim_{r \to \infty} \frac{\sum_{\chi \in G(R_{3,p^r}) \setminus G(R_{2,p^r})} f(\Theta_\chi)}{\#G(R_{3,p^r}) \setminus G(R_{2,p^r})} = \int_{U(2)} f(U) \, dU,
\]

(1.10)
where \( dU \) is the unit mass Haar measure on \( U(2) \); such a result is known as an equidistribution result. For \( p = 5 \), Katz showed that (1.10) fails. For \( p = 2 \) he remarked [Kat13] Rem. 5.2 that he suspects that (1.10) fails as well. Lemma 5.5 confirms this suspicion. Indeed, taking \( f(U) = |\text{Tr}(U^{24})|^2 \), the left hand side of (1.10) is 4 since \( \Theta_{\chi}^{24} = I_2 \) for \( \chi \in G(R_3, 2^\ell \backslash G(R_2, 2^\ell)) \), while the right hand side is 2 by [DE01 Thm. 2.1].

An interpretation of Lemma 5.5 in terms of supersingularity of certain curves associated with cyclotomic function fields is given in [6].

Throughout the paper, we use the following notation. For any \( k \in \mathbb{N}_{>0} \) we define
\[
\omega_k = e^{\frac{2\pi ik}{p^k}}.
\]

For a prime power \( q = p^r \), we denote by \( \chi_q: \mathbb{F}_q \to \mathbb{C}^\times \) the additive character defined by
\[
\chi_q(a) = \omega_p^{\text{Tr}_{q/p}(a)}
\]
for all \( a \in \mathbb{F}_q \).

\section{2 Short interval characters}

In \( \mathbb{F}_q(T) \), the prime at infinity is not different from any other prime of degree 1. In particular, one may define Dirichlet characters modulo a power of the prime at infinity. We call these characters “short interval characters” and review their properties below. We follow Hayes [Hay65], who studied the Dirichlet characters of \( \mathbb{F}_q(T) \) in an elementary manner.

\subsection*{2.1 Equivalence relation}

For any \( \ell \in \mathbb{N} \) we define an equivalence relation \( R_\ell \) on \( \mathcal{M}_q \) by saying that \( A \equiv B \) mod \( R_\ell \) if and only if \( A \) and \( B \) have the same first \( \ell \) next-to-leading coefficients. We sometimes write \( R_{\ell,q} \) instead of \( R_\ell \), to emphasize that we work in \( \mathcal{M}_q \).

We say that \( A \in \mathcal{M}_q \) is invertible modulo \( R_\ell \) if there exists \( B \in \mathcal{M}_q \) such that \( AB \equiv 1 \) mod \( R_\ell \). It can be shown that any element of \( \mathcal{M}_q \) is invertible modulo \( R_\ell \).

Consider the set \( \mathcal{M}_q/R_\ell \) of equivalence classes of \( R_\ell \). It can be shown that \( \mathcal{M}_q/R_\ell \) is an abelian group with respect to polynomial multiplication, having as identity element the equivalence class of the polynomial 1. The group \( \mathcal{M}_q/R_\ell \) is a \( p \)-group of order \( q^\ell \).

We sometimes represent an element \( T^n + a_1T^{n-1} + \ldots + a_n \in \mathcal{M}_q/R_\ell \) by an \( \ell \)-tuple \( (a_1, a_2, \ldots, a_\ell) \). In this notation, multiplication of elements of \( \mathcal{M}_q/R_\ell \) takes the form
\[
(a_1, \ldots, b_\ell)(b_1, \ldots, b_\ell) = (a_1 + b_1, a_2 + a_1 b_2 + b_2, \ldots, a_\ell + \sum_{i+j=\ell, 1 \leq i, j \leq \ell-1} a_i b_j + b_\ell).
\]
The \( j \)-th coordinate of \( (a_1, \ldots, a_\ell)^k \) is the coefficient of \( T^{nk-j} \) in \( (T^n + a_1 T^{n-1} + a_2 T^{n-2} + \ldots)^k \):
\[
(a_1, \ldots, a_\ell)^k = \left( k \atop 1 \right) a_1 + \left( k \atop 1 \right) a_2 + \left( k \atop 2 \right) a_1^2 + \left( k \atop 1 \right) a_3 + 2 \left( k \atop 2 \right) a_1 a_2 + \left( k \atop 3 \right) a_1^3 + \ldots + \left( k \atop 1 \right) a_\ell + \ldots.
\]

\subsection*{2.2 Characters}

For every character \( \chi \) of the finite abelian group \( \mathcal{M}_q/R_\ell \), we define \( \chi^\dagger \) with domain \( \mathcal{M}_q \) as follows: For a given \( A \in \mathcal{M}_q \), if \( \epsilon \) is the equivalence class of \( A \), then
\[
\chi^\dagger(A) = \chi(\epsilon).
\]
The functions \( \chi^\dagger \) defined in this way are called the characters of the relation \( R_\ell \), or simply characters modulo \( R_\ell \). We denote by \( G(R_\ell) \) the set containing them:
\[
G(R_\ell) = \{ \chi^\dagger : \chi \in \mathcal{M}_q/R_\ell \}.
\]
We will often abuse notation and write \( \chi \) instead of \( \chi^\dagger \). In particular, we denote by \( \chi_0 \) the trivial character in \( G(R_\ell) \).
Assume that \( \ell > 0 \). A character modulo \( R_\ell \) is said to be “primitive modulo \( R_\ell \)”, or just “primitive”, if \( \chi \notin G(R_{\ell-1}) \).

We have a natural restriction map from \( \mathcal{M}_q/R_\ell \) to \( \mathcal{M}_q/R_{\ell-1} \), which in particular implies that \( G(R_{\ell-1}) \) may be considered as a subgroup of \( G(R_\ell) \).

If \( n \geq \ell \) and \( \chi \in G(R_\ell) \), then a consequence of the orthogonality relations in \( \mathcal{M}_q/R_\ell \) is

\[
\frac{1}{q^n} \sum_{F \in \mathcal{M}_{n,q}} \chi(F) = \begin{cases} 
0 & \text{if } \chi \neq \chi_0, \\
1 & \text{if } \chi = \chi_0.
\end{cases}
\]

(2.1)

### 2.3 L-functions

Let \( \chi \) be a character of \( G(R_\ell) \). The \( L \)-function of \( \chi \) is the following power series in \( u \):

\[
L(u, \chi) = \sum_{f \in \mathcal{M}_q} \chi(f) u^{\deg f},
\]

which also admits the Euler product

\[
L(u, \chi) = \prod_{P \in \mathcal{M}_q} (1 - \chi(P) u^{\deg P})^{-1}.
\]

If \( \chi \) is the trivial character \( \chi_0 \), then

\[
L(u, \chi) = \frac{1}{1 - qu}.
\]

Otherwise, (2.1) implies that \( L(u, \chi) \) is a polynomial in \( u \) of degree at most \( \ell - 1 \).

Weil’s proof of the Riemann Hypothesis for Function Fields [Wei74, Thm. 6, p. 134] implies the Riemann Hypothesis for the \( L \)-functions of \( \chi \in G(R_\ell) \), as shown explicitly by Rhin [Rhi72, Thm. 3] in his thesis (cf. [EH91, Thm. 5.6] and the discussion following it). Hence we know that if we factor \( L(u, \chi) \) as

\[
L(u, \chi) = \prod_{i=1}^{\deg L(u, \chi)} (1 - \gamma_i(\chi) u),
\]

then the \( \gamma_i(\chi) \)'s are \( q \)-Weil numbers of weight 1, i.e. they are algebraic numbers such that

\[
|\gamma_i(\chi)| = \sqrt{q}.
\]

(2.2)

and (2.2) is true for the conjugates of \( \gamma_i(\chi) \) as well. The functional equation for \( L(u, \chi) \) implies that if \( \chi \) is primitive modulo \( R_\ell \) then

\[
\deg L(u, \chi) = \ell - 1.
\]

We use the notation \( \gamma_i(\chi) \) for the inverse roots of \( L(u, \chi) \) throughout this paper.

### 2.4 Lifts of characters

Let \( \sigma : F_{q^\ell} \to F_{q^\ell} \) be the Frobenius automorphism \( \sigma(a) = a^q \), which generates \( \text{Gal}(F_{q^\ell}/F_q) \). We extend \( \sigma \) to an automorphism of \( F_q[T] \) by \( \sigma(\sum_i a_i T^i) = \sum_i \sigma(a_i) T^i \). For every \( A \in F_{q^\ell}[T] \), the polynomial

\[
N^{(\ell)}(A) = \prod_{i=1}^{\deg A} \sigma^i(A)
\]

is called the norm of \( A \) relative to \( F_q[T] \). As explained in [Hay65, Thm. 2.2] for example, \( N^{(\ell)}(A) \) is a polynomial in \( F_q[T] \). In addition, the map \( A \mapsto N^{(\ell)}(A) \) is multiplicative. It is also true that if \( A \equiv B \mod R_{\ell,q} \) then \( N^{(\ell)}(A) \equiv N^{(\ell)}(B) \mod R_{\ell,q} \), i.e. the \( \ell \) next-to-leading coefficients of the norm of \( A \) depend only on the \( \ell \) next-to-leading coefficients of \( A \). If \( \chi \in G(R_{\ell,q}) \), then for every \( A \in F_{q^\ell}[T] \) we define

\[
\chi^{(\ell)}(A) = \chi(N^{(\ell)}(A)).
\]

For every character \( \chi \) of \( R_{\ell,q} \), \( \chi^{(\ell)} \) is a character of \( R_{\ell,q^\ell} \). The map \( \chi \mapsto \chi^{(\ell)} \) is a homomorphism from \( G(R_{\ell,q}) \) to \( G(R_{\ell,q^\ell}) \) [Hay65, Thm. 5.2]. By [Hay65, Thm. 9.2], if \( L(u, \chi) = \prod_{i=1}^{\deg L(u, \chi)} (1 - \gamma_i(\chi) u) \) then

\[
L(u, \chi^{(\ell)}) = \prod_{i=1}^{\deg L(u, \chi)} (1 - \gamma_i(\chi)^\ell u).
\]

(2.3)

The character \( \chi^{(\ell)} \) is called a lift of \( \chi \) to \( F_{q^\ell} \).
2.5 Formula for $\psi_q$

The following lemma gives a classical exact formula for $\psi_q$ [Hay65, Thms. 6.1, 9.2].

**Lemma 2.1.** Let $n \in \mathbb{N}_{>0}$ and $\ell \in \mathbb{N}$. Let $t_1, \ldots, t_\ell \in \mathbb{F}_q$. Set

$$A = (t_1, t_2, \ldots, t_\ell) \in \mathcal{M}_q/R_\ell.$$

For any $\chi_0 \neq \chi \in G(R_\ell)$, let $\{\gamma_i(\chi)\}_{i=1}^{\deg L(u, \chi)}$ be the inverse roots of $L(u, \chi)$. Then

$$\psi_q(n, t_1, \ldots, t_\ell) = q^{n-\ell} - \frac{1}{q} \sum_{\chi \neq \chi_0 \in G(R_\ell)} \chi(A) \sum_{i=1}^{\deg L(u, \chi)} \gamma_i^n(\chi).$$

Lemma 2.1 implies that for fixed $\ell$ and $q$, only a finite collection of complex numbers governs the behavior of the function $\psi_q(n, t_1, \ldots, t_\ell)$, namely the multisets $\{\gamma_i(\chi)\}_{\chi \in G(R_\ell)}$. For instance, the formulas for $\psi_q(n, t_1, t_2, t_3)$ given in [YM04, Thm. 4] and [FY03, Thm. 3.4] may be recovered easily by a computation of 10 complex numbers: two inverse roots for each $\chi \in G(R_3)/G(R_2)$ and one inverse root for each $\chi \in G(R_2)/G(R_1)$.

**Remark 2.2.** From Lemma 2.1 and the Riemann Hypothesis for $\chi \in G(R_\ell)$, (1.15) is obtained.

2.6 The groups $\mathcal{M}_q/R_\ell$ and $G(R_\ell)$

Let $q = p^l$ be a prime power. The groups $\mathcal{M}_q/R_\ell$ and $G(R_\ell)$ are abelian $p$-groups of order $q^{\ell}$. They are isomorphic since $G(R_{\ell})$ is the character group of $\mathcal{M}_q/R_\ell$.

The decomposition of $\mathcal{M}_q/R_\ell$ as a product of cyclic $p$-groups is known, see for instance Katz [Kat13, Sec. 2] or Fomenko [Fom96, p. 276]. We only need the following simpler result.

**Lemma 2.3.** Let $q = p^l$ be a prime power and $\ell \geq 1$. The exponent $e_q$ of $\mathcal{M}_q/R_\ell \cong G(R_\ell)$ is

$$e_q = p^{\lceil \log_p(\ell+1) \rceil}.$$  

**Proof.** The exponent of $\mathcal{M}_q/R_\ell$ is necessarily a power of $p$. For $A \in \mathcal{M}_q/R_\ell$, the power $A^p$ has first $p^\ell - 1$ next-to-leading coefficients equal to zero. Hence, a sufficient condition for $A^p^\ell = 1$ is $p^\ell - 1 \geq \ell$.

Let $t$ be the smallest integer satisfying (2.4), that is, $t = \lceil \log_p(\ell+1) \rceil$. Then $(T+1)^{p^\ell-1} = T^{p^\ell-1} + 1 \neq 1 \mod R_\ell$, which proves that $p^\ell$ is the exponent of the group.

When $p > \ell$, the $L$-functions of the characters in $G(R_{\ell,q})$ have a simple description given in the following lemma. The $L$-functions are essentially $L$-functions of Artin-Schreier curves.

**Lemma 2.4.** Let $q = p^l$ be a prime power. Let $\ell$ be a positive integer such that $p > \ell$. Let $\chi \in G(R_{\ell,q})$. Then there exist unique constants $\lambda_1, \ldots, \lambda_\ell \in \mathbb{F}_q$ such that

$$\chi(a_1, \ldots, a_\ell) = \chi_q \left( \sum_{j=1}^\ell \lambda_j \cdot [T^j] \log(1 + a_1 T + a_2 T^2 + \ldots + a_\ell T^\ell) \right)$$

(2.5)

for all $a_i \in \mathbb{F}_q$. Conversely, any function on $\mathcal{M}_q/R_\ell$ defined as in (2.5) is an element of $G(R_{\ell,q})$.

Here $[T^j] \log(1 + a_1 T + a_2 T^2 + \ldots + a_\ell T^\ell)$ denotes the coefficient of $T^j$ in the formal power series $\log(1 + a_1 T + a_2 T^2 + \ldots + a_\ell T^\ell)$. As $j \leq \ell < p$, this coefficient is well defined.

This lemma is implicit in the works of Katz and Fomenko mentioned above. We supply a proof for completeness.

**Proof.** The characters of $\mathbb{F}_q^\ell$ are given by $(b_1, \ldots, b_\ell) \mapsto \chi_q(\sum_{j=1}^\ell \lambda_j b_j)$ for $\lambda_i \in \mathbb{F}_q$. The lemma is deduced by observing that $\mathcal{M}_q/R_\ell$ is isomorphic to $\ell \mathbb{F}_q$ under

$$T^\ell + a_1 T^{\ell-1} + \ldots + a_\ell \mapsto \log(1 + a_1 T + \ldots + a_\ell T^\ell) \mod T^{\ell+1},$$

(2.6)

where $\log(1 + a_1 T + \ldots + a_\ell T^\ell) \mod T^{\ell+1}$ is a truncation of $\log$, well defined since $j \leq \ell < p$. The fact that (2.6) is an isomorphism follows from the fact that $\log$ turns multiplication into addition. The fact that it is an isomorphism follows from the fact that we have an explicit inverse, given by (a truncation of) the exponential map.
3 Periodicity and symmetry for $p = 2, \ell = 3$

3.1 Symmetries of sums involving roots of unity

The following lemma describes some symmetries of expressions involving roots of unity.

**Lemma 3.1.** Let $m_1, m_2$ be positive integers with $m_2 \mid m_1$. Let $F_1, \ldots, F_{m_1} \in \mathbb{Q}[x]$. Let $S : \mathbb{Z}^2 \to \mathbb{C}$ be the function defined by

$$S(k_1, k_2) = \sum_{i=1}^{m_1} \omega_{m_1}^{ik_1} F_i(\omega_{m_2}^{k_2}).$$

Assume that, for all $k_1, k_2 \in \mathbb{Z}$,

$$S(k_1, k_2) \in \mathbb{Q}. \quad (3.1)$$

Then the following hold.

1. The function $S(k_1, k_2)$ is periodic in $k_1$ with period $m_1$ and in $k_2$ with period $m_2$.
2. For any $\lambda \in \mathbb{Z}$ such that $(\lambda, m_1) = 1$, we have

$$S(k_1, k_2) = S(\lambda k_1, \lambda k_2). \quad (3.2)$$

3. Let $k_1, k_2 \in \mathbb{Z}$. Let $d$ be any integer such that $d \equiv (k_1, m_1)^{-1} \mod (k_1, m_1)$ and $(d, m_1) = 1$. Then

$$S(k_1, k_2) = S((k_1, m_1), dk_2).$$

**Proof.** The first part is trivial. For the second part, let $\sigma_\lambda : \mathbb{Q}(\omega_{m_1}) \to \mathbb{Q}(\omega_{m_1})$ be the field automorphism fixing $\mathbb{Q}$ defined by

$$\sigma_\lambda(\omega_{m_1}) = \omega_{m_1}^\lambda.$$

We have

$$\sigma_\lambda(S(k_1, k_2)) = S(\lambda k_1, \lambda k_2).$$

From (3.1) and (3.2), we deduce the second part of the lemma. To establish the third part, choose in the second part $\lambda = d$ and use the periodicity of $S(k_1, k_2)$ in $k_1$. \qed

3.2 Periodicity and symmetry for $\ell = 1, 2$

We first consider $\psi_q(n, t_1, \ldots, t_\ell)$ for $\ell = 1$. Let $q = p^r$ be a prime power and let $\chi \in G(R_1)$ be a non-trivial character. Then $\deg L(u, \chi) \leq 1 - 1$. Hence

$$L(u, \chi) = 1.$$

In particular, $L(u, \chi)$ has no roots. Applying Lemma 2.1 with $\ell = 1$, we obtain that

$$\psi_q(n, t_1) = q^{n-1}, \quad (3.3)$$

a result first proved by Carlitz [Car52, Eq. 6.1]. In particular, $\frac{\psi_q(n, t_1) - q^{n-1}}{q^{n/2}}$ has period 1 in $n$ for any $t_1 \in \mathbb{F}_q$.

In Proposition 3.2 we prove some periodicity and symmetry properties of $\psi_q(n, t_1, t_2)$. Although these properties follow from the exact formulas for $\psi_q(n, t_1, t_2)$ obtained by Kuz’min, we take a different route. We do this because similar ideas are used in the proof of Theorem 1.1, which is a natural sequel to Proposition 3.2.

**Proposition 3.2.** Let $q = p^r$ be a prime power. Let $t_1, t_2 \in \mathbb{F}_q$ and define

$$f_q(n, t_1, t_2) = \frac{\psi_q(n, t_1, t_2) - q^{n-2}}{q^{n/2}}.$$

Then the following hold.
1. The function \( f_q \) may be written as

\[
f_q(n, t_1, t_2) = \frac{-1}{q^2} \sum_{\chi \in G(R_2) \setminus G(R_1)} \chi(t_1, t_2) \left( \frac{\gamma_1(\chi)}{\sqrt{q}} \right)^n,
\]

where

\[
\gamma_1(\chi) = -\sum_{a \in \mathbb{F}_q} \chi(T + a).
\]

2. Let

\[
a_q = \begin{cases} 
4p & \text{if } 2 \nmid r \text{ and } p \nmid 1 \mod 4, \\
2p & \text{otherwise.}
\end{cases}
\]

Then \( \gamma_1(\chi) \) is a root of unity of order dividing \( a_q \). Moreover, if \( a_q = 4p \) then the order of \( \frac{\gamma_1(\chi)}{\sqrt{q}} \) is divisible by \( (a_q, 8) \).

3. The function \( f_q(n, t_1, t_2) \) has period \( a_q \) in \( n \in \mathbb{N}_{>0} \). Additionally, the following symmetries hold. Let \( n \in \mathbb{N}_{>0} \). If \( \lambda \in \mathbb{N}_{>0} \) satisfies \( (\lambda, 2p) = 1 \), then

\[
f_q(n, t_1, t_2) = f_q \left( \lambda n, \lambda t_1, \lambda t_2 + \left( \frac{\lambda}{2} \right) t_1^2 \right),
\]

and if \( d \in \mathbb{Z} \) satisfies \( (d, 2p) = 1 \) and \( d \equiv (\frac{n}{(m, o_q)})^{-1} \mod \frac{o_q}{(m, o_q)} \), then

\[
f_q(n, t_1, t_2) = f_q \left( (n, o_q), dt_1, dt_2 + \left( \frac{d}{2} \right) t_1^2 \right).
\]

The proof we give for the second part of Proposition 3.2 is essentially due to Katz [Katz13, p. 3631], although Katz was only interested in odd \( p \).

**Proof.** The first part of the proposition follows directly from Lemma 2.1 with \( \ell = 2 \). We proceed to prove the second part. We start by showing that \( \gamma_1(\chi) \) has absolute value \( \sqrt{q} \) whenever \( \chi \in G(R_2) \setminus G(R_1) \).

We have

\[
|\gamma_1(\chi)|^2 = \gamma_1(\chi)\overline{\gamma_1(\chi)} = \sum_{a, b \in \mathbb{F}_q} \chi(T + a)\overline{\chi(T + b)} = \sum_{a, b \in \mathbb{F}_q} \chi(T + a)\overline{\chi(T^2 - bT + b^2)}
\]

\[
= \sum_{a, b \in \mathbb{F}_q} \chi(-b + a, b(b - a)) = \sum_{a' = a - b, b' = b - a \in \mathbb{F}_q} \chi(a', a'b').
\]

We observe that the terms in the last sum of (3.4) corresponding to some fixed \( a' \neq 0 \) contribute \( \sum_{c \in \mathbb{F}_q} \chi(a', c) \) to the sum. Hence, (3.4) may be written as follows.

\[
|\gamma_1(\chi)|^2 = \sum_{a' \neq 0 \in \mathbb{F}_q} \chi(a', c) + \sum_{b' \in \mathbb{F}_q} \chi(0, 0) = \sum_{x, y \in \mathbb{F}_q} \chi(x, y) - \sum_{c \in \mathbb{F}_q} \chi(0, c) + q. \tag{3.5}
\]

We have

\[
\sum_{x, y \in \mathbb{F}_q} \chi(x, y) = 0 \tag{3.6}
\]

by the orthogonality relation (2.1). The identity \( \chi(a, b) = \chi(a, 0) \cdot \chi(0, b) \) implies that \( \chi \) cannot be constant 1 on the subgroup \( \{ (0, c) : c \in \mathbb{F}_q \} \subseteq \mathcal{M}_q/R_2 \), since otherwise \( \chi \in G(R_1) \). Hence, orthogonality of characters implies that

\[
\sum_{c \in \mathbb{F}_q} \chi(0, c) = 0. \tag{3.7}
\]

From (3.5), (3.6) and (3.7) we get that

\[
|\gamma_1(\chi)| = q. \tag{3.8}
\]

Let

\[
e_q = \begin{cases} 
p & \text{if } p > 2, \\
2p & \text{if } p = 2,
\end{cases}
\]

9
be the exponent of the group $G(R_{2,q})$, according to Lemma 2.3. Since $\chi(a, b)^{e_\sigma} = \chi((a, b)^{e_\sigma}) = \chi(0, 0) = 1$, it follows that $\chi(a, b) \in \mathbb{Z}[\omega_{eq}]$ and so

$$\gamma_1(\chi), \gamma_2(\chi) \in \mathbb{Z}[\omega_{eq}].$$

(3.9)

Since the image of $\chi$ is contained in $\mathbb{Z}[\omega_{eq}]$, $\sigma \circ \chi$ is a character of $G(R_2) \setminus G(R_1)$ for any $\sigma \in \text{Gal}(\mathbb{Q}(\omega_{eq})/\mathbb{Q})$. Repeating the arguments that gave us (3.8) we obtain

$$|\gamma_1(\sigma \circ \chi)| = |\sigma(\gamma_1(\chi))| = \sqrt{q}$$

(3.10)

for all $\sigma \in \text{Gal}(\mathbb{Q}(\omega_{eq})/\mathbb{Q})$. Let $p$ be the unique prime in $\mathbb{Z}[\omega_{eq}]$ lying over $p$. From (3.8) and (3.9), $\gamma_1(\chi)$ is an algebraic integer with $|\gamma_1(\chi)|_q = 1$ for any finite prime $q$ in $\mathbb{Q}(\omega_{eq})$, except for $p$. Set

$$g_p = \left\{ \begin{array}{ll}
\sum_{a \in \mathbb{F}_p} \left( \frac{a}{p} \right) \omega_p^a & \text{if } p > 2 \in \mathbb{Z}[\omega_{eq}], \\
1 + i & \text{if } p = 2.
\end{array} \right.$$

Since $g_p$ is a quadratic Gauss sum when $p > 2$, we have \[HR00\] Ch. 6, Thm. 1)

$$g_p = \sqrt{p} \cdot \begin{cases} 
1 & \text{if } p \equiv 1 \mod 4, \\
i & \text{if } p \equiv 3 \mod 4, \\
\sqrt{2} = \omega_8 & \text{if } p = 2.
\end{cases}$$

(3.11)

In particular,

$$|g_p| = \sqrt{p}.$$  

(3.12)

Let

$$c_\chi = \frac{\gamma_1(\chi)}{g_p} \in \mathbb{Q}(\omega_{eq}).$$

Since $g_p$ is an algebraic integer in $\mathbb{F}_p$, it follows that $|c_\chi|_q = 1$ for all finite primes $q$ in $\mathbb{Q}(\omega_{eq})$, except possibly at $p$. As $|\sigma(\gamma_1(\chi))| = |g_p| = \sqrt{q}$ for all $\sigma \in \text{Gal}(\mathbb{Q}(\omega_{eq})/\mathbb{Q})$ by (3.10) and (3.12), it follows that $|c_\chi|_q = 1$ at the infinite primes also. Thus, the product formula $1 = \prod_q c_\chi(q)$ implies that $|c_\chi|_p = 1$. Hence $c_\chi$ is an algebraic integer, in fact a unit in $\mathbb{Z}[\omega_{eq}]$.

A result of Kronecker \[Kro57\] states that if all the conjugates of an algebraic integer have absolute value 1, then it is a root of unity. Applying this result to $c_\chi$ shows that $c_\chi$ is a root of unity. The roots of unity in $\mathbb{Q}(\omega_{eq})$ are powers of $\omega_{eq}(1+1_{p \geq 2})$. Hence, for any $\chi \in G(R_2) \setminus G(R_1)$,

$$\exists j \in \mathbb{N} : \frac{\gamma_1(\chi)}{\sqrt{q}} = \omega_{eq}^{o_{\chi,A}(1+1_{p \geq 2})} \cdot \left( \frac{g_p}{\sqrt{p}} \right)^r.$$  

(3.13)

Combining (3.11) and (3.13), the second part of the proposition follows.

We turn to the last part of the proposition. For any $A = (t_1, t_2) \in R_{2,q}$ and $\chi \in G(R_2)/G(R_1)$, the number $\chi(A)$ is a root of unity of order (dividing) $e_q$, hence we may write

$$\chi(A) = \omega_{eq}^{a_{\chi,A}^q},$$

where $a_{\chi,A}$ is an integer satisfying $0 \leq a_{\chi,A} < e_q$. For any $0 \leq i < e_q$, let

$$F_i(x) = \frac{-1}{q^2} \sum_{\chi \in G(R_2) \setminus G(R_1)} \frac{\gamma_1(\chi)}{\sqrt{q}} \omega_{eq}^{i a_{\chi,A}} x^{a_{\chi,A}}.$$  

Set $m_1 = o_q, m_2 = e_q$ and define the following function from $\mathbb{Z}^2$ to $\mathbb{C}$:

$$S(k_1, k_2) = \sum_{i=1}^{m_1} \omega_{eq}^{ik_1} F_i(\omega_{eq}^{k_2}).$$

We have

$$S(k_1, k_2) = \frac{-1}{q^2} \sum_{i=1}^{o_q} \sum_{\chi \in G(R_2) \setminus G(R_1)} \frac{\gamma_1(\chi)}{\sqrt{q}} \omega_{eq}^{i} \omega_{eq}^{a_{\chi,A}}$$

$$= \frac{-1}{q^2} \sum_{\chi \in G(R_2) \setminus G(R_1)} \left( \frac{\gamma_1(\chi)}{\sqrt{q}} \chi(A)^{k_2} \right)$$

$$= f_q \left( k_1, k_2 t_1, k_2 t_2 + \frac{k_2^2}{2} t_1^2 \right).$$
Fomenko has shown, by elementary means, that the Proposition 3.3

Properties of $G$ Hypothesis [Fom96, Prop. 5]. He did so by using a certain homomorphism implied by (3.14), allows us to recover

We recall the definition and properties of $\varepsilon$ in the proof of Theorem 1.1. Let $\chi$ and reduces the problem to the evaluation of $\psi$

The third part of the lemma now follows by applying Lemma 3.1 to $S$. □

Remark 3.3. Let $q = 2^r$. Proposition 3.2 may be used in order to calculate $\psi_q(n, t_1, t_2)$ explicitly, which recovers [Kuz89] Thms. 2–4. Namely, the third part of the proposition shows that the calculation of $\psi_q(n, t_1, t_2)$ reduces to the following cases: $n = 1, 2, 4$, and if $2 \nmid r$ then also the case $n = 8$. The cases $n = 1, 2$ are trivial. By Proposition 3.2 we can treat $n = 8$ as follows.

$$\frac{\psi_q(8, t_1, t_2) - q^6}{q^4} = -\frac{1}{q^2} \sum_{\chi \in G(R_3) \setminus G(R_1)} \chi(t_1, t_2) \left( \frac{\gamma_1(\chi)}{\sqrt{q}} \right)^8 = -\frac{1}{q^2} \sum_{\chi \in G(R_2) \setminus G(R_1)} \chi(t_1, t_2)$$

$$= -\frac{1}{q^2} \sum_{\chi \in G(R_2)} \chi(t_1, t_2) + \frac{1}{q^2} \sum_{\chi \in G(R_1)} \chi(t_1, t_2)$$

$$= -1_{(t_1, t_2) = (0, 0)}^\varepsilon + \frac{1_{t_1 = 0}}{q}.$$ 

So the only non-trivial case is $n = 4$. An appropriate linear change of variables $f(T) \mapsto \frac{f(\lambda_1 T + \lambda_2)}{\chi_2}$ ($\lambda_1 \in \mathbb{F}_q^\times$ and $\lambda_2 \in \mathbb{F}_q$) shows that

$$\psi_q(4, a, b) = \begin{cases} 
\psi_q(4, 1, 0) & \text{if } a \neq 0, \\
\psi_q(4, 0, 1) & \text{if } a = 0, b \neq 0, \\
\psi_q(4, 0, 0) & \text{if } a = b = 0,
\end{cases} \quad (3.14)$$

and reduces the problem to the evaluation of $\psi_q(4, 1, 0)$, $\psi_q(4, 0, 1)$ and $\psi_q(4, 0, 0)$. The values $\psi_q(4, 0, 0)$ and $\psi_q(4, 0, 1)$ are calculated in [Kuz89] Thm. 1, Prop. 2–3] by elementary considerations. The relation

$$q^4 = \psi_q(4) = \sum_{a,b \in \mathbb{F}_q} \psi_q(4, a, b) = \psi_q(4, 0, 0) + (q - 1)\psi_q(4, 0, 1) + (q^2 - q)\psi_q(4, 1, 0),$$

implied by (3.14), allows us to recover $\psi_q(4, 1, 0)$ as well.

3.3 Properties of $G(R_{3,2^r})$

Fomenko has shown, by elementary means, that the $L$-functions of $\chi \in G(R_{3,2^r})$ satisfy the Riemann Hypothesis [Fom96, Prop. 5]. He did so by using a certain homomorphism

$$\varepsilon: G(R_{3,2^r}) \mapsto \mathbb{F}_{2^r}. \oplus \mathbb{F}_{2^r}.$$ We recall the definition and properties of $\varepsilon$, as proven in [Fom96, Prop. 5], because we build upon them in the proof of Theorem 3.1. Let $q = 2^r$. Let $a, b, c, d \in \mathbb{F}_q$. In $\mathcal{M}_q/R_3$ we have

$$(0, a, b) \cdot (0, c, d) = (0, a + b, c + d),$$

hence $H(R_{3,q}) = \{(0, a, b) : a, b \in \mathbb{F}_q\}$ is a subgroup of $\mathcal{M}_q/R_3$, isomorphic to $\mathbb{F}_q \oplus \mathbb{F}_q$. The restriction $\chi_H$ of any character $\chi \in G(R_{3,q})$ to $H$ is a character of $H$, given by

$$\chi_H(0, a, b) = \chi_q(\lambda a + \mu b)$$

for some unique $\lambda, \mu \in \mathbb{F}_q$. Fomenko defined the homomorphism $\varepsilon: G(R_{3,q}) \mapsto \mathbb{F}_q \oplus \mathbb{F}_q$ by

$$\varepsilon(\chi) = (\lambda, \mu).$$

Proposition 3.4 (Fomenko). Let $q = 2^r$. Let $\chi \in G(R_{3,q})$ and assume that $\varepsilon(\chi) = (\lambda, \mu)$.

1. The homomorphism $\varepsilon$ is surjective and its kernel is of size $q$.

2. If $\lambda = \mu = 0$ then $\chi \in G(R_1)$. If $\mu = 0$ but $\lambda \neq 0$ then $\chi \in G(R_2) \setminus G(R_1)$.

3. If $\mu \neq 0$ then $\chi \in G(R_3) \setminus G(R_2)$. If we write the $L$-function of $\chi$ as

$$L\left(\frac{u}{\sqrt{q}}, \chi\right) = 1 + \alpha(\chi)u + \beta(\chi)u^2,$$
then
\[ \alpha(\chi)^2 = \chi \left( \frac{\lambda}{\mu}, 0, 0 \right) + \sum_{c \in \mathbb{F}_q: \mu c^3 + \lambda c^2 + 1 = 0} \chi(c, 0, 0) \]
and
\[ \beta(\chi) = \chi \left( \frac{\lambda}{\mu}, 0, 0 \right). \]

4. If \( \chi \) is primitive modulo \( R_3 \) then \( L(u, \chi) \) satisfies the Riemann Hypothesis.

The proof of Theorem 1.1 relies crucially on the following lemma.

**Lemma 3.5.** Let \( q = 2^r \). Let \( \chi \) be a primitive character modulo \( R_{3,q} \). If we factor \( L(u, \chi) \) as
\[ (1 - \gamma_1(\chi)u)(1 - \gamma_2(\chi)u). \]
then
\[ \frac{\gamma_1(\chi)}{\sqrt{4}} \]
are roots of unity of order (dividing) 24.

**Proof.** Let \( \lambda, \mu \in \mathbb{F}_q \) be the elements such that \( \varepsilon(\chi) = (\lambda, \mu) \). We know that \( \mu \neq 0 \), as \( \chi \) is primitive. The polynomial
\[ F(x) = \mu x^3 + \lambda x^2 + 1 \]
is separable, since \( (F, F') = (F, \mu x^2) = 1 \). Let \( \sqrt{\chi(\frac{\lambda}{\mu}, 0, 0)} \) be some quadratic root of \( \chi(\frac{\lambda}{\mu}, 0, 0) \). By Proposition 3.4 we have
\[ G(u) := L \left( \frac{u}{\sqrt{q \cdot \chi(\frac{\lambda}{\mu}, 0, 0)}}, \chi \right) = 1 + \sqrt{S_{\chi} u + u^2}, \]
where \( \sqrt{S_{\chi}} \) is one of the quadratic roots of
\[ S_{\chi} = 1 + \frac{\sum_{c \in \mathbb{F}_q: \mu c^3 + \lambda c^2 + 1} \chi(c, 0, 0)}{\chi(\frac{\lambda}{\mu}, 0, 0)}. \]
By the Riemann Hypothesis for \( L(u, \chi) \), we must have that \( S_{\chi} \) is real and
\[ S_{\chi} \geq 0, \]
since \( \sqrt{S_{\chi}} \) is a sum of a number on the unit circle and its complex conjugate.

The group \( M_{\eta}/R_{3,q} \) has exponent 4. Hence \( \sqrt{\chi(\frac{\lambda}{\mu}, 0, 0)} \) is a root of unity of order (dividing) 4, and so its square roots are roots of unity of order (dividing) 8, which divides 24. So we can reduce the lemma to showing that the roots of \( G(u) \) are roots of unity of order dividing 24.

1. If \( F(x) = 0 \) has no roots in \( \mathbb{F}_q \) then \( S_{\chi} = 1 \) and \( G(u) = 1 \pm u + u^2 | u^6 - 1 \). In particular, the roots of \( G \) are roots of unity of order dividing 24.
2. If \( F(x) = 0 \) has exactly one solution in \( \mathbb{F}_q \) then \( S_{\chi} \in \{1 + a : a \in \mu_4\} \). The two complex options \( 1 \pm i \) are impossible, hence we have \( G(u) = 1 + u^2 \) or \( G(u) = 1 + \sqrt{2}u + u^2 | u^4 + 1 | u^8 - 1 \). In either case, the roots of \( G \) are roots of unity of order dividing 24.
3. If \( F(x) = 0 \) has exactly two solutions in \( \mathbb{F}_q \), namely \( c_1 \) and \( c_2 \), we reach a contradiction since Vieta’s formulas and separability of \( F \) guarantee that \( \frac{\lambda}{\mu} + c_1 + c_2 \) is a third distinct solution to \( F(x) = 0 \).
4. If \( F(x) = 0 \) has three distinct solutions in \( \mathbb{F}_q \), then \( S_{\chi} \in \{1 + a + b + c : a, b, c \in \mu_4\} \). We know that \( S_{\chi} \) is real and \( \geq 0 \), which leaves us only the options
\[ S_{\chi} \in \{0, 2, 4\}. \]
Hence \( G(u) = 1 + u^2 \) or \( G(u) = 1 \pm \sqrt{2}u + u^2 | u^4 + 1 \) or \( G(u) = 1 \pm 2u + u^2 = (u \pm 1)^2 \). In all cases the roots of \( G \) are roots of unity of order dividing 24.

Regardless of the number of solutions to \( F(x) = 0 \) in \( \mathbb{F}_q \), the lemma is proven. \( \square \)
3.4 Proof of Theorem 1.1

Let \( q = 2^r \). From Lemma 2.4 we may write

\[
f_q(n, t_1, t_2, t_3) = \frac{-1}{q^3} \sum_{\chi \neq \chi \in G(R_3)} \chi(t_1, t_2, t_3) \sum_{j=1}^{\deg L(u, \chi)} \left( \frac{\gamma_j(\chi)}{\sqrt{q}} \right)^n.
\] (3.15)

Proposition 3.2 and Lemma 3.5 tell us that \( \gamma_j(\chi) \) are roots of unity of order dividing 24. Fix \( A = (t_1, t_2, t_3) \in M_q/R_3, q \). By Lemma 2.3 the group \( M_q/R_3, q \) has exponent 4. Hence, for any \( \chi \neq \chi \in G(R_3) \), the number \( \chi(A) \) is a root of unity of order dividing 4. Thus we may write

\[
\chi(A) = \omega_4^{a_{\chi, A}},
\]

where \( a_{\chi, A} \) is an integer satisfying \( 0 \leq a_{\chi, A} < 4 \). For any \( 0 \leq i < 24 \), let

\[
F_i(x) = \frac{-1}{q^3} \sum_{\chi \neq \chi \in G(R_3)} \sum_{1 \leq j \leq \deg L(u, \chi)} \sum_{\gamma_j(\chi) \in \omega_4} x^{a_{\chi, A}}.
\]

Set \( m_1 = 24 \), \( m_2 = 4 \) and define the following function from \( Z^2 \) to \( \mathbb{C} \):

\[
S(k_1, k_2) = \sum_{i=1}^{m_1} \omega_{m_1}^{ik_1} F_i(\omega_{m_2}^{ik_2}).
\]

As \( A^{k_2} = (k_2 t_1, t_2, t_3 + \frac{k_2}{2} t_1) \), we have by (3.15)

\[
S(k_1, k_2) = \frac{-1}{q^3} \sum_{\chi \neq \chi \in G(R_3)} \sum_{1 \leq j \leq \deg L(u, \chi)} \sum_{\gamma_j(\chi) \in \omega_4} \omega_{24}^{ik_1} \omega_4^{a_{\chi, A}}
\]

\[
= \frac{-1}{q^3} \sum_{\chi \neq \chi \in G(R_3)} \chi(A^{k_2}) \sum_{1 \leq j \leq \deg L(u, \chi)} \left( \frac{\gamma_j(\chi)}{\sqrt{q}} \right)^{k_1}
\]

\[
= f_q \left( k_1, k_2 t_1, k_2 t_2 + \frac{k_2}{2} t_1, k_2 t_3 + \frac{k_2}{3} t_1 \right).
\]

The theorem now follows by applying Lemma 3.1 to \( S \).

\[ \square \]

3.5 Proof of Corollary 1.5

Let \( q = 2^r \). Let \( t_1, t_2, t_3 \in \mathbb{F}_q \). For any \( \chi \neq \chi \in G(R_3) \) and any inverse root \( \gamma \) of \( L(u, \chi) \), Proposition 3.2 and Lemma 3.5 tell us that \( \frac{\gamma_j(\chi)}{\sqrt{q}} \) is a root of unity of order dividing 24. Thus, Lemma 2.1 implies that

\[
f_q(24, t_1, t_2, t_3) = \frac{-1}{q^3} \sum_{\chi \neq \chi \in G(R_3)} \chi(t_1, t_2, t_3) \sum_{j=1}^{\deg L(u, \chi)} \left( \frac{\gamma_j(\chi)}{\sqrt{q}} \right)^{24}
\]

\[
= \frac{-1}{q^3} \sum_{\chi \neq \chi \in G(R_3)} \chi(t_1, t_2, t_3) \sum_{j=1}^{\deg L(u, \chi)} 1
\]

\[
= \frac{-1}{q^3} \left( \sum_{\chi \in G(R_3)} \chi(t_1, t_2, t_3) + 2 \sum_{\chi \in G(R_3)} \chi(t_1, t_2, t_3) \right).
\] (3.16)

By (2.1) we have

\[
\sum_{\chi \in G(R_3)} \chi(t_1, t_2, t_3) = q \cdot 1_{t_1=0},
\]

\[
\sum_{\chi \in G(R_3)} \chi(t_1, t_2, t_3) = q^2 \cdot 1_{t_1=t_2=0},
\]

\[
\sum_{\chi \in G(R_3)} \chi(t_1, t_2, t_3) = q^3 \cdot 1_{t_1=t_2=t_3=0}.
\] (3.17)

Substituting (3.17) in (3.16), we conclude the proof of the corollary.

\[ \square \]
4 Periodicity and symmetry for $p = 5$, $\ell = 3$

4.1 Auxiliary lemmas

**Lemma 4.1.** Let $q = p^r$ be a prime power with $p \geq 5$. Let $\chi \in G(R_3, q) \setminus G(R_2, q)$. Then there exist $a \in \mathbb{F}_q^\times$, $b, c \in \mathbb{F}_q$ such that

$$L \left( \frac{u}{\sqrt{q} \omega_p^r}, \chi \right) = 1 + \sum_{x \in \mathbb{F}_q} \chi(x) \left( ax^3 + bx \right) + u^2.$$

Moreover, if $\lambda_1, \lambda_2, \lambda_3 \in \mathbb{F}_q$ are the constants associated with $\chi$ in Lemma 2.4, then we may take

$$a = \frac{\lambda_3}{3}, \quad b = \lambda_1 - \frac{\lambda_2^2}{4\lambda_3}.$$

**Proof.** By applying Lemma 2.4 with $\ell = 3$ we get that there are $\lambda_1, \lambda_2, \lambda_3 \in \mathbb{F}_q$ such that

$$L(u, \chi) = 1 + g_1(\lambda_1, \lambda_2, \lambda_3)u + g_2(\lambda_1, \lambda_2, \lambda_3)u^2,$$

where

$$g_1(\lambda_1, \lambda_2, \lambda_3) = \sum_{x \in \mathbb{F}_q} \chi(x) \left( \lambda_1 x - \frac{1}{2} \lambda_2 x^2 + \frac{1}{3} \lambda_3 x^3 \right),$$

$$g_2(\lambda_1, \lambda_2, \lambda_3) = \sum_{x \in \mathbb{F}_q} \chi(x) \left( \lambda_1 x + \lambda_2 (y - \frac{1}{2} x^2) + \lambda_3 \left( \frac{1}{3} x^3 - xy \right) \right),$$

and $\lambda_3 \neq 0$ (otherwise $\chi \in G(R_2)$). As observed by Fomenko [Rom96, p. 269], we may simplify $g_2$ as follows:

$$g_2(\lambda_1, \lambda_2, \lambda_3) = \sum_{x \in \mathbb{F}_q} \chi(x) \left( \lambda_1 x - \frac{1}{2} \lambda_2 x^2 + \frac{1}{3} \lambda_3 x^3 \right) \left( \sum_{y \in \mathbb{F}_q} \chi(y) (\lambda_2 - \lambda_3 y) \right)$$

$$= q \cdot \chi \left( \lambda_1 \lambda_2 - \frac{1}{2} \lambda_2 \left( \frac{\lambda_2}{\lambda_3} \right)^2 + \frac{1}{3} \lambda_3 \left( \frac{\lambda_2}{\lambda_3} \right)^3 \right)$$

$$= q \cdot \chi \left( \frac{\lambda_1 \lambda_2}{\lambda_3} - \frac{1}{6} \lambda_3^2 \right).$$

In particular,

$$L \left( \frac{u}{\sqrt{q} \omega_p^r}, \chi \right) = 1 + \sum_{x \in \mathbb{F}_q} \chi(x) \left( \lambda_1 x - \frac{1}{2} \lambda_2 x^2 + \frac{1}{3} \lambda_3 x^3 \right) \left( \sum_{y \in \mathbb{F}_q} \chi(y) \frac{\lambda_1 \lambda_2}{\lambda_3} - \frac{1}{6} \lambda_3^2 \right) u^2.$$

Let $c \in \mathbb{F}_p$ such that $\omega_p^r = \chi \left( \frac{\lambda_1 \lambda_2}{\lambda_3} - \frac{1}{6} \lambda_3^2 \right)$. A short calculation reveals that

$$L \left( \frac{u}{\sqrt{q} \omega_p^r}, \chi \right) = 1 + \sum_{x \in \mathbb{F}_q} \chi(x) \left( \lambda_1 x - \frac{1}{2} \lambda_2 x^2 + \frac{1}{3} \lambda_3 x^3 \right) \left( \lambda_1 = \frac{\lambda_2}{\lambda_3} \right) \left( \lambda_1 - \frac{\lambda_2^2}{\lambda_3^2} \right) u^2$$

$$= 1 + \frac{\sum_{x \in \mathbb{F}_q} \chi(x) \left( \lambda_1 = \frac{\lambda_2}{\lambda_3} \right) \left( \lambda_1 - \frac{\lambda_2^2}{\lambda_3^2} \right) u^2}{\sqrt{q}}.$$

This establishes the lemma with $a = \frac{\lambda_3}{3}$, $b = \lambda_1 - \frac{\lambda_2^2}{4\lambda_3}$, as needed. \hfill \Box

We need the following lemma, which is essentially a special case of a result of van der Geer and van der Vlugt [VdGVdV92, Thm. 13.7].

**Lemma 4.2.** Let $p = 5$ and $q = p^r$. Let $\chi \in G(R_3, q) \setminus G(R_2, q)$. Then the roots of $L \left( \frac{u}{\sqrt{q} \omega_p^r}, \chi \right)$ are roots of unity of order dividing 60.
Proof. Let \( a, b \in F_q, a \neq 0 \). By Lemma 4.1 it suffices to show that

\[
S = \sum_{x \in F_q} \chi_{\phi^i}(ax^3 + bx)
\]  

(4.1)

is of the form \( 5^{r/2}(\omega_{60}^i + \omega_{60}^{-i}) \) for some \( i \). Van der Geer and van der Vlugt proved that the Artin-Schreier curve

\[
C_{a,b} : y^5 - y = ax^6 + bx^2
\]

is supersingular, which implies that [Kat05, Lem. 3.8.4]

\[
\overline{C}_{a,b} : y^5 - y = ax^3 + bx
\]

is also supersingular. Supersingularity of \( \overline{C}_{a,b} \) implies that the zeros of its zeta function

\[
Z_{\overline{C}_{a,b}}(u) = \frac{\prod_{i=1}^4 L_i(u)}{(1 - qu)(1 - u)}
\]

are roots of unity divided by \( \sqrt{q} \), where \( L_j(u) = \exp(\sum_{i \geq 1}(\sum_{x \in F_q} \chi_{\phi^i}(j(ax^3 + bx)))u^i/i) \). The linear coefficient of \( L_1 \) is \( S \), \( \deg L_1 = 2 \), and the same argument as in Lemma 4.1 shows that the leading coefficient of \( L_1 \) is \( q \). Thus \( \frac{S}{q} \) is a sum of two roots of unity, the roots of \( L_1(\frac{1}{\sqrt{q}}) \):

\[
S = -5^{r/2}(\omega + \omega^{-1}).
\]  

(4.2)

By (4.1) and (4.2), \( \omega + \omega^{-1} \) is a (real) element of \( Q(\omega_5, \sqrt{5}) = Q(\omega_5) \). If \( \omega \) is a primitive root of unity of order \( d \), then comparing degrees in the inclusions \( Q \subseteq Q(\omega + \omega^{-1}) \subseteq Q(\omega_5) \) we obtain \( \phi(d) | 2\phi(5) = 8 \). A finite check shows that we must have \( d | 60 \), as needed, or \( 8 | d \), which contradicts the inclusion since \( Q(\omega_8 + \omega_8^{-1}) = Q(\sqrt{2}) \not\subseteq Q(\omega_5) \).

4.2 Proof of Theorem 1.2

Let \( q = 5^r \). From Lemma 2.4 we may write

\[
f_q(n, t_1, t_2, t_3) = \frac{-1}{q^3} \sum_{\chi_0 \neq \chi \in G(R_3)} \chi(t_1, t_2, t_3) \sum_{j=1}^{\deg L(u, \chi)} \left( \frac{\gamma_j(\chi)}{\sqrt{q}} \right)^n.
\]

Fix \( A = (t_1, t_2, t_3) \in M_q/R_3,q \). The group \( M_q/R_3,q \) has exponent 5. Hence, for any \( \chi \in G(R_3)/G(R_1) \), the number \( \chi(A) \) is a root of unity of order (dividing) 5. Thus we may write

\[
\chi(A) = \omega_{5}^{a_{\chi,A}},
\]

where \( a_{\chi,A} \) is an integer satisfying \( 0 \leq a_{\chi,A} < 5 \). For any \( 0 \leq i < 60 \), let

\[
F_i(x) = \frac{-1}{q^3} \sum_{\chi_0 \neq \chi \in G(R_3)} \sum_{1 \leq j \leq \deg L(u, \chi)} x^{a_{\chi,A}}.
\]

Set \( m_1 = 60, m_2 = 5 \) and define the following function from \( Z^2 \) to \( \mathbb{C} \):

\[
S(k_1, k_2) = \sum_{i=1}^{m_1} \omega_{5}^{ik_1} F_i(\omega_{5}^{k_2}).
\]

Note that

\[
S(k_1, k_2) = \frac{-1}{q^3} \sum_{i=1}^{60} \sum_{\chi_0 \neq \chi \in G(R_3)} \sum_{1 \leq j \leq \deg L(u, \chi)} \omega_{60}^{ik_1} \omega_{5}^{k_2 a_{\chi,A}}
\]

\[
= \frac{-1}{q^3} \sum_{\chi_0 \neq \chi \in G(R_3)} \chi(A^{k_2}) \sum_{1 \leq j \leq \deg L(u, \chi)} \left( \frac{\gamma_j(\chi)}{\sqrt{q}} \right)^{k_1}
\]

\[
= f_q \left( k_1, k_2 t_1, k_2 t_2 + \frac{k_2}{2} t_1^2, k_2 t_3 + k_2 (k_2 - 1) t_1 t_2 + \left( \frac{k_2}{3} \right) t_1^3 \right).
\]

Applying Lemma 3.4 to \( S \), we deduce that (1.6), (1.7), (1.8) hold. \( \square \)
4.3 Proof of Corollary 1.6

Let \( q = 5^r \). Let \( t_1, t_2, t_3 \in \mathbb{F}_q \). For any \( \chi \neq \chi \in G(R_3) \) and any inverse root \( \gamma \) of \( L(u, \chi) \), Proposition 3.2 and Lemma 1.2 tell us that \( \frac{\alpha}{\gamma} \) is a root of unity of order dividing 60. From this point we proceed as in 4.3, with 24 replaced with 60. \( \square \)

5 A non-periodicity result

5.1 Auxiliary lemmas

Lemma 5.1. Let \( \alpha_1, \ldots, \alpha_m \in \mathbb{C} \) be non-zero complex numbers. Define the following sequence:

\[
a_n = \sum_{i=1}^{m} \alpha_i^n, \quad (n \geq 1).
\]

The sequence \( \{a_n\}_{n \geq 1} \) is periodic in \( n \) if and only if all the \( \alpha_i \)-s are roots of unity.

Proof. This follows immediately from two observations: Firstly, the generating function \( \sum_{n \geq 1} a_n x^n = \sum_{i=1}^{m} \frac{\alpha_i x}{1-\alpha_i x} \) has poles at the \( \alpha_i^{-1} \)-s, and at them only. Secondly, the generating function of a sequence with period \( N \) has poles at some subset of the roots of unity of order dividing \( N \), and vice versa. \( \square \)

Lemma 5.2. Let \( p \) be a prime \( \geq 7 \). Let \( j \in \mathbb{F}_p^* \) and \( \varepsilon_1, \varepsilon_2 \in \{\pm 1\} \). Then there exists \( i \in \mathbb{F}_p \) such that

\[
\left( \frac{i-j}{p} \right) = \varepsilon_1, \quad \left( \frac{i+j}{p} \right) = \varepsilon_2,
\]

where \( \left( \frac{\cdot}{p} \right) \) is the Legendre symbol modulo \( p \). For \( p = 5 \) it can happen that (5.1) has no solution in \( i \).

Proof. We begin with the case \( p \geq 7 \). Consider the following sum:

\[
S(\varepsilon_1, \varepsilon_2) = \sum_{i \in \mathbb{F}_p} \left( 1 + \varepsilon_1 \left( \frac{i-j}{p} \right) \right) \left( 1 + \varepsilon_2 \left( \frac{i+j}{p} \right) \right).
\]

Each term of the sum \( S(\varepsilon_1, \varepsilon_2) \) has value in \( \{0, 2, 4\} \). By counting how often each value is achieved, we find that

\[
S(\varepsilon_1, \varepsilon_2) = 4 \cdot \# \{i \in \mathbb{F}_p : \left( \frac{i-j}{p} \right) = \varepsilon_1, \left( \frac{i+j}{p} \right) = \varepsilon_2 \} + 2 \cdot 1(\varepsilon_1 = \varepsilon_2) + 2 \cdot 1(\varepsilon_1 \neq \varepsilon_2) = 4 \cdot \# \{i \in \mathbb{F}_p : \left( \frac{i-j}{p} \right) = \varepsilon_1, \left( \frac{i+j}{p} \right) = \varepsilon_2 \} + 2 \cdot 1(\varepsilon_1 = \varepsilon_2) + 2 \cdot 1(\varepsilon_1 \neq \varepsilon_2).
\]

On the other hand, we may expand \( S(\varepsilon_1, \varepsilon_2) \) and get that

\[
S(\varepsilon_1, \varepsilon_2) = p + \varepsilon_1 \sum_{i \in \mathbb{F}_p} \left( \frac{i-j}{p} \right) + \varepsilon_2 \sum_{i \in \mathbb{F}_p} \left( \frac{i+j}{p} \right) + \varepsilon_1 \varepsilon_2 \sum_{i \in \mathbb{F}_p} \left( \frac{i^2-j^2}{p} \right) = p + 0 + 0 - \varepsilon_1 \varepsilon_2 = 4 \cdot \# \{i \in \mathbb{F}_p : \left( \frac{i-j}{p} \right) = \varepsilon_1, \left( \frac{i+j}{p} \right) = \varepsilon_2 \} + 2 \cdot 1(\varepsilon_1 = \varepsilon_2) + 2 \cdot 1(\varepsilon_1 \neq \varepsilon_2).
\]

Comparing (5.2) and (5.3), we get that

\[
4 \cdot \# \{i \in \mathbb{F}_p : \left( \frac{i-j}{p} \right) = \varepsilon_1, \left( \frac{i+j}{p} \right) = \varepsilon_2 \} \geq p - \varepsilon_1 \varepsilon_2 - 2 - 2 \geq p - 5 > 0,
\]

which shows that there exists \( i \in \mathbb{F}_p \) as required. We conclude the proof by observing that for \( p = 5 \), there is no \( i \in \mathbb{F}_p \) such that

\[
\left( \frac{i-2}{5} \right) = 1, \quad \left( \frac{i+2}{5} \right) = 1.
\]

holds. \( \square \)

Lemma 5.3. Let \( p \geq 7 \) be a prime. Let \( \chi \in G(R_{3, p}) \setminus G(R_{2, p}) \), and let \( \lambda_1, \lambda_2, \lambda_3 \in \mathbb{F}_p \) be the constants associated with \( \chi \) in Lemma 2.4. If \( p \equiv 2 \mod 3 \) and \( \lambda_2^2 - 4 \lambda_1 \lambda_3 = 0 \), then the roots of \( L(\chi, \chi) \) are roots of unity. Otherwise, both roots of \( L(\chi, \chi) \) are not roots of unity.
Proof. From Lemma 4.1 we have

$$L\left(\frac{u}{\sqrt{p}}\omega_p^i\right) = 1 + \sum_{x \in \mathbb{F}_p} \chi_p(ax^3 + bx)$$

for \(a = \frac{\lambda_1}{\sqrt{p}} \in \mathbb{F}_p^*, \ b = \lambda_1 - \frac{\lambda_2^2}{\sqrt{p}}\) and some \(c \in \mathbb{F}_p\). We first assume that \(p \equiv 2 \mod 3\) and that \(\lambda_2^2 - 4\lambda_1 \lambda_3 = 0\). This implies that \(b = 0\) and that the map \(x \mapsto ax^3\) is a permutation of \(\mathbb{F}_p\). Thus, \(\sum_{x \in \mathbb{F}_p} \chi_p(ax^3 + bx) = 0\) and the roots of \(L\left(\frac{u}{\sqrt{p}}\right)\) are both roots of unity.

From now on we assume that either \(p \equiv 1 \mod 3\) or that \(\lambda_1 - \frac{\lambda_2^2}{\lambda_3} \neq 0\) holds. Assume for contradiction’s sake that some root of \(L\left(\frac{u}{\sqrt{p}}\right)\) is a root of unity. The second root of \(L\left(\frac{u}{\sqrt{p}}\right)\) must also be a root of unity, since the product of the two roots is a root of unity. Let \(\omega_n^i, \omega_n^{-i}\) be the roots of \(L\left(\frac{u}{\sqrt{p}}\right)\), where \((i, n) = 1\).

Consider

$$S = \sum_{x \in \mathbb{F}_p} \chi_p(ax^3 + bx)$$

The quadratic Gauss sum \(g_p = \sum_{a \in \mathbb{F}_p} \left(\frac{a}{p}\right)\omega_p^a\) satisfies \(g_p \in \mathbb{Q}(\omega_p)\) and \(g_p^2 = (-1)^{\frac{p-1}{2}}\) \([R90]\) Prop. 6.3.2].

Thus we have

$$S \in \mathbb{Q}(\omega_p, \sqrt{p}) = \mathbb{Q}(\omega_{tp}), \quad t = \begin{cases} 1 & \text{if } p \equiv 1 \mod 4, \\ 4 & \text{if } p \equiv 3 \mod 4. \end{cases}$$

Moreover, \(S\) is real since \(\omega_n^i + \omega_n^{-i}\) is real, hence it follows from (5.5) that in fact

$$S \in \mathbb{Q}(\omega_{tp} + \omega_{tp}^{-1}).$$

Since \(S\) generates \(\mathbb{Q}(\omega_n + \omega_n^{-1})\), we have from (5.9) that

$$\mathbb{Q}(\omega_n + \omega_n^{-1}) \subseteq \mathbb{Q}(\omega_{tp} + \omega_{tp}^{-1}).$$

We have

$$\mathbb{Q}(\omega_n + \omega_n^{-1}) = \mathbb{Q}(\omega_n + \omega_n^{-1}) \cap \mathbb{Q}(\omega_{tp} + \omega_{tp}^{-1}) \subseteq \mathbb{Q}(\omega_n) \cap \mathbb{Q}(\omega_{tp}) = \mathbb{Q}(\omega_{n, tp}).$$

Since \(\mathbb{Q}(\omega_n + \omega_n^{-1}) \subseteq \mathbb{R}\), (5.7) implies that

$$\mathbb{Q}(\omega_n + \omega_n^{-1}) = \mathbb{Q}(\omega_{n, tp} + \omega_{n, tp}^{-1})$$

If \(n = 1\) or \(n = 2\), (5.8) is trivial. If \(n > 2\), by comparing degrees over \(\mathbb{Q}\), (5.8) implies that

$$\phi(n) = \phi(n, tp),$$

which in turn implies that \(n \mid tp\). Both for \(n = 1, 2\) and \(n > 2\), we have

$$n \mid 2(2, t)p.$$

If \(p \equiv 1 \mod 4\) then \(n \mid 2p\), hence for some \(j \in \mathbb{Z}\) we have

$$\omega_n^i + \omega_n^{-i} = \pm(\omega_p^j + \omega_p^{-j}), \quad \sqrt{p} = \sum_{i \in \mathbb{F}_p} \left(\frac{i}{p}\right) \omega_p^i.$$  

Plugging (5.9) in (5.10) we get

$$\sum_{x \in \mathbb{F}_p} \chi_p(ax^3 + bx) = \pm(\omega_p^j + \omega_p^{-j}) \sum_{i \in \mathbb{F}_p} \left(\frac{i}{p}\right) \omega_p^i$$

$$= \pm \sum_{i \in \mathbb{F}_p} \left(\frac{i}{p}\right) (\omega_p^{i+j} + \omega_p^{i-j}).$$

If \(p \equiv 3 \mod 4\) then \(n \mid 4p\), hence for some \(j, k \in \mathbb{Z}\) we have

$$\omega_n^i + \omega_n^{-i} = \omega_p^j \omega_4^k + \omega_p^{-j} \omega_4^{-k}, \quad \sqrt{p} = -\omega_4 \sum_{i \in \mathbb{F}_p} \left(\frac{i}{p}\right) \omega_p^i.$$  

17
Plugging (5.11) in (5.4) we get
\[
\sum_{x \in F_p} \chi_p(ax^3 + bx) = \omega_4 \left( \omega_p^{ij} + \omega_p^{-j} \right) \sum_{i \in F_p} \left( \frac{i}{p} \right) \omega_p^i.
\] (5.12)

If \( k \) is even, (5.12) shows that \( \omega_4 \in \mathbb{Q}(\omega_p) \), a contradiction. Hence we may assume that \( k \) is odd. In this case (5.12) is equivalent to
\[
\sum_{x \in F_p} \chi_p(ax^3 + bx) = \pm (\omega_p^j - \omega_p^{-j}) \left( \sum_{i \in F_p} \left( \frac{i}{p} \right) \omega_p^i \right)
\] (5.13)

The only non-trivial linear relation among \( \{ \omega_p^i : 0 \leq i \leq p-1 \} \) is that their sum is 0. Hence, we may compare the coefficient of \( \omega_p^i \) in both sides of (5.10) (if \( p \equiv 1 \mod 4 \)) or of (5.13) (if \( p \equiv 3 \mod 4 \)), up to some constant \( \lambda \in \mathbb{C} \). This gives us the following equality for all \( i \in F_p \):
\[
\#\{ x \in F_p : ax^3 + bx = i \} = \lambda + \varepsilon_1 \left( \frac{i-j}{p} \right) + \varepsilon_2 \left( \frac{i+j}{p} \right),
\] (5.14)

where \( \lambda \) is some complex number and \( \varepsilon_1, \varepsilon_2 \in \{ \pm 1 \} \) satisfy
\[
\varepsilon_1 \varepsilon_2 = \begin{cases} 
1 & \text{if } p \equiv 1 \mod 4, \\
-1 & \text{if } p \equiv 3 \mod 4.
\end{cases}
\]

Summing (5.14) over all \( i \in F_p \) we see that necessarily \( \lambda = 1 \). If \( j \neq 0 \), then Lemma 5.2 shows that there exists \( i \in F_p \) such that \( \left( \frac{i-j}{p} \right) = -\varepsilon_1 \), \( \left( \frac{i+j}{p} \right) = -\varepsilon_2 \), in which case the right hand side of (5.14) is negative while the left hand side is non-negative, which gives a contradiction. Thus, we must have \( j = 0 \).

If \( j = 0 \) and \( p \equiv 1 \mod 4 \), then for any \( i \in F_q \) such that \( \left( \frac{i}{p} \right) = -\varepsilon_1 = -\varepsilon_2 \) we get that the right hand side of (5.14) is equal to \(-1\), while the left hand side is non-negative, which gives a contradiction. Thus, we must have \( j = 0 \) and \( p \equiv 3 \mod 4 \). In that case, \( \varepsilon_1 = -\varepsilon_2 \) and (5.14) simplifies to
\[
\#\{ x \in F_p : ax^3 + bx = i \} = 1
\]
for all \( i \in F_p \), which means that \( ax^3 + bx \) is a permutation polynomial on \( F_p \). Dickson classified permutation polynomials of degree 3 [Dic58, p. 63], and in characteristic \( > 3 \) they exist only when \( p \equiv 2 \mod 3 \) and are given by \( a_1(x + a_2)^3 + a_3 \). By assumption, either \( p \equiv 1 \mod 3 \), in which case we do not have permutation polynomials, or \( b \neq 0 \), in which case \( ax^3 + bx \) is not of the form \( a_1(x + a_2)^3 + a_3 \). We reach a contradiction, hence our assumption is wrong and none of the roots of \( L(u/\sqrt{q}, \chi) \) is a root of unity. □

### 5.2 Proof of Theorem 1.3

By Lemma 2.1 we have the following formula for \( f_{q,\ell}(n) \):
\[
f_{q,\ell}(n) = -q^{-\ell} \sum_{\chi \neq \chi_0 \in G(R_{\ell,q})} \deg L(u, \chi) \sum_{i=1}^{R \equiv q} \left( \frac{\gamma_i(\chi)}{\sqrt{q}} \right)^n,
\]
where \( \gamma_i(\chi) \)-s are the inverse roots of \( L(u, \chi) \). Lemma 5.1 shows that \( f_{q,\ell}(n) \) is not periodic if and only if there is some \( \chi \neq \chi_0 \in G(R_{\ell,q}) \) such that at least one the ratios \( \gamma_i(\chi)/\sqrt{q} \) is not a root of unity. So our aim is to prove that such a character exists in all the cases of Theorem 1.3. If \( q = p^\ell \), then it is in fact enough to prove the existence of such a character for \( q = p \), since given \( \chi \neq \chi_0 \in G(R_{\ell,q}) \) such that at least one the ratios \( \gamma_i(\chi)/\sqrt{p} \) is not a root of unity, we may take its lift \( \chi^{(r)} \in G(R_{\ell,q}) \) to \( \mathbb{F}_q \), and (2.13) guarantees that \( L(u/\sqrt{p^\ell}, \chi^{(r)}) \) also has a root which is not a root of unity. This is what we show now.

1. \( p = 2 \), \( \ell \geq 4 \): Lemma 2.3 shows that the group \( \mathcal{M}_2/R_4 \) is isomorphic to \((\mathbb{Z}/8\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})\) (the unique abelian group of order 16 and exponent equal to 8). It is generated, for example, by the elements
Let \( C \) be a prime power. A curve \( C \) defined over \( \mathbb{F}_p \) is called supersingular if its Jacobian is isogenous to a product of supersingular elliptic curves. This condition is known to be the same as saying that the \( p \)-adic L-function of \( C \) has two roots which are not even algebraic integers.

The relations
\[
(0, 1, 0, 0) = (1, 0, 0, 0)^2, \quad (0, 1, 1, 0) = (1, 0, 0, 0)^2(0, 0, 1, 0),
\]
\[
(1, 0, 1, 0) = (1, 0, 0, 0)^3(0, 0, 1, 0), \quad (1, 1, 0, 0) = (1, 0, 0, 0)^2(0, 0, 1, 0),
\]
\[
(1, 1, 1, 0) = (1, 0, 0, 0)^3
\]
imply that
\[
L\left(\frac{u}{\sqrt{2}}, \chi\right) = 1 + \frac{1 + \omega_8}{\sqrt{2}} u + \frac{1 + \omega_8}{\sqrt{2}} u^2 + \omega_8 u^3 = (1 + iu)(1 + (\frac{1 + \omega_8}{\sqrt{2}} - i)u - \omega_8iu^2),
\]
which has two roots which are not even algebraic integers.

2. \( p = 3, \ell \geq 3 \): Lemma 2.3 shows that the group \( \mathcal{M}_3/R_3 \) is isomorphic to \((\mathbb{Z}/9\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})\) (the unique abelian group of order 27 and exponent equal to 9). It is generated, for example, by the elements \( T + 1 \) and \( T^2 + 1 \) of order 9 and 3, respectively. Consider the character \( \chi \in G(R_{3,3}) \setminus G(R_{2,3}) \subseteq G(R_{2,3}) \) defined by
\[
\chi(1,0,0) = \omega_9, \quad \chi(0,1,0) = 1.
\]
The relations
\[
(2, 0, 0) = (1, 0, 0)^3(0, 0, 1, 0)^2, \quad (0, 2, 0) = (0, 1, 0)^2,
\]
\[
(1, 2, 0) = (1, 0, 0)^2(0, 1, 0), \quad (1, 1, 0) = (1, 0, 0)^2(0, 1, 0)^2,
\]
\[
(2, 2, 0) = (1, 0, 0)^5(0, 1, 0)
\]
imply that
\[
L\left(\frac{u}{\sqrt{3}}, \chi\right) = 1 + \frac{1 + \omega_9 + \omega_5}{\sqrt{3}} u + u^2,
\]
which has two roots which are not even algebraic integers.

3. \( p = 5, \ell \geq 4 \): By taking \( \ell = 4, \lambda_1 = \lambda_2 = \lambda_3 = 0, \lambda_4 = 1 \) in Lemma 2.4 we get that the following function is a character of \( R_{4,5} \):
\[
\chi(a_1, a_2, a_3, a_4) = \omega_5^{a_1^2 + a_2^2 - a_1a_3 - \frac{a_2^2}{2} + a_4}.
\]
The \( L \)-function of \( \chi \) is
\[
L\left(\frac{u}{\sqrt{5}}, \chi\right) = 1 + \frac{1 + 4\omega_5}{\sqrt{5}} u - \frac{1 + 4\omega_5^4}{\sqrt{5}} u^2 - u^3 = (1 + u)(1 + \frac{1 - \sqrt{5} + 4\omega_5}{\sqrt{5}} u - u^2),
\]
which has two roots which are not roots of unity.

4. \( p \geq 7, \ell \geq 3 \): This case is treated in Lemma 5.3 which shows that if \( p \equiv 1 \text{ mod } 3 \) we may take any \( \chi \in G(R_{3,p}) \setminus G(R_{2,p}) \), and if \( p \equiv 2 \text{ mod } 3 \) then most choices of \( \chi \in G(R_{3,p}) \setminus G(R_{2,p}) \) work.

\[ \square \]

6 Supersingular curves

Let \( q = p^n \) be a prime power. A curve \( C \) defined over \( \mathbb{F}_q \) is called supersingular if its Jacobian is isogenous to a product of supersingular elliptic curves. This condition is known to be the same as saying that the roots of the zeta function of \( C \),
\[
Z_C(u) = \exp\left(\sum_{n \geq 1} \frac{\# C(\mathbb{F}_{q^n})u^n}{n}\right),
\]

are of the form $\sqrt{7}$ times of root of unity.

We use an analogue of cyclotomic fields in finite fields, due to Carlitz [Car38] and Hayes [Hay74], and we follow Rosen [Ros02, Ch. 12] in our notation. For a given $\ell \geq 1$, we consider the following fields. Let $K_\ell = \mathbb{F}_q(T)(\ell)$ be the abelian extension of $\mathbb{F}_q(T)$ obtained by adjoining the $T^{\ell-1}$-torsion elements of the Carlitz module $\Lambda$. The extension $K_\ell / \mathbb{F}_q(T)$ is totally ramified at the prime at infinity, and unramified everywhere else. We have $[K_\ell : \mathbb{F}_q(T)] = q^{\ell-1}$, and $K_\ell$ has a unique subfield $L_\ell$ with $[L_\ell : \mathbb{F}_q(T)] = q'$, which is called the maximal real subfield of $K_\ell$. The Dedekind zeta function of $L_\ell$ factors as the product of $L(u, \chi)$ for $\chi \in G(R_{\ell,q})$, after completing these $L$-functions at the prime at infinity. This is because the Dirichlet characters $G(R_{\ell,q})$ can be considered as the representations of $\text{Gal}(L_\ell/\mathbb{F}_q(T))$. The field $L_\ell$ is the function field of a certain smooth projective curve, which we denote by $C_\ell$. The Dedekind zeta function of $L_\ell$ is the same the zeta function of $C_\ell$, so that

$$Z_{C_\ell}(u) = \prod_{\chi \in G(R_{\ell,q})} L^*(u, \chi).$$

(6.1)

Here $L^*$ is the completed $L$-function. As $\chi \in G(R_{\ell,q})$ vanishes on the prime at infinity unless $\chi$ is trivial, we have

$$L^*(u, \chi) = \begin{cases} 
L(u, \chi) & \text{if } \chi_0 \neq \chi \in G(R_\ell), \\
L(u, \chi)(1-u)^{-1} & \text{if } \chi = \chi_0.
\end{cases}$$

From Lemma 2.1 and (6.1), it follows that

$$\psi_q(n, 0, \ldots, 0) = \frac{\#C_\ell(\mathbb{F}_q^n) - 1}{q^\ell}.$$ 

The number

$$\pi_q(n, 0, \ldots, 0)$$

can be interpreted as the number of primes in $\mathbb{F}_q[T]$ of degree $n$ that split completely in $L_\ell$. Let $g$ be the genus of $C_\ell$. As $Z_{C_\ell}(u) = P_{C_\ell}(u)/(1 - q'u(1 - u))$ where $P_{C_\ell}$ is a polynomial of degree $2g$, and $\deg L(u, \chi) = k$ if $\chi \in G(R_{k,q}) \setminus G(R_{k-1,q})$, (6.1) implies that

$$2g = \sum_{k=1}^\ell (k-1)(q^k - q^{k-1}) = (\ell-1)q^\ell - (q + q^2 + \ldots + q^{\ell-1}).$$

Note that $C_1$ is of genus 0. By Proposition 3.2, $C_2$ is supersingular. By Theorem 1.3, $C_3$ is supersingular if and only if $p \in \{2, 5\}$, and $C_4$ is not supersingular for $\ell \geq 4$.

Finally we explain how to write an equation for an affine model of $C_\ell$. Define $g_0(X) \in \mathbb{F}_q(T)[X]$ recursively by $g_0(X) = 1$, $g_0(X) = X^q + \frac{1}{T}$, $g_{n+1}(X) = g_n(X)^q + \frac{g_n(X)}{T}$. The irreducible polynomial generating $K_\ell$ is $\frac{g_{\ell+1}(X)}{g_1(X)}$, which is a function field analogue of a cyclotomic polynomial. Induction shows that $g_i(X) = Xh_i(X^{q-1})$ for a unique $h_i \in \mathbb{F}_q(T)[X]$, and so $\frac{g_{\ell+1}(X)}{g_1(X)} = \frac{h_{\ell+1}}{h_1}(X^{q-1})$. As $[K_\ell : L_\ell] = q - 1$, we find that $L_\ell$ is the splitting field of $\frac{h_{\ell+1}}{h_1}(X)$. So $\frac{h_{\ell+1}}{h_1}(X) = 0$ is an affine model for $C_\ell$. For instance, a short calculation gives the following affine model for $C_1$:

$$\sum_{i=1}^q X^i \left(\frac{-1}{T}\right)^{q-i} + \frac{1}{T} = 0.$$ 

Acknowledgments

I thank Zé’ev Rudnick for useful discussions, Lior Bary-Soroker for suggesting Lemma 6.1 and an anonymous referee for constructive comments. I was supported by the European Research Council under the European Union’s Seventh Framework Programme (FP7/2007-2013) / ERC grant agreement no 320755.
A Computing $\pi_q$ from $\psi_q$

A.1 Möbius inversion

We explain how exact formulas for $\psi_q(n, t_1, \ldots, t_\ell)$ yield exact formulas for $\pi_q(n, t_1, \ldots, t_\ell)$. We introduce the following notation. For a given arithmetic function

$$\alpha: \mathcal{M}_q \to \mathbb{C}$$

and a positive integer $\ell$, we attach a summatory function

$$S_{\alpha, \ell}: \mathbb{N}_{>0} \times \mathcal{M}_q / R_\ell \to \mathbb{C}$$

defined by

$$S_{\alpha, \ell}(n, A) = \sum_{f \in \mathcal{M}_{n, q}, f \equiv A \text{ mod } R_\ell} \alpha(f).$$

In this notation,

$$\psi_q(n, t_1, \ldots, t_\ell) = S_{\Lambda_q, \ell}(n, (t_1, \ldots, t_\ell)),$$

$$\pi_q(n, t_1, \ldots, t_\ell) = S_{1_{\mathbb{P}_q}, \ell}(n, (t_1, \ldots, t_\ell)).$$

Lemma A.1. Let $n, \ell$ be two positive integers. Let $A \in \mathcal{M}_{n, q}$. We have

$$S_{1_{\mathbb{P}_q}, \ell}(n, A) = \frac{\sum_{d|n} \mu(d) \sum_{B \in \mathcal{M}_q / R_\ell, B^d \equiv A \text{ mod } R_\ell} S_{\Lambda_q, \ell}(\frac{n}{d}, B)}{n}. \quad (A.1)$$

Proof. We may write $S_{1_{\mathbb{P}_q}, \ell}(n, A), S_{\Lambda_q, \ell}(n, A)$ as sums over primes of degree dividing $n$:

$$S_{1_{\mathbb{P}_q}, \ell}(n, A) = \sum_{d|n} \sum_{P \in \mathbb{P}_q, \deg P = d} 1_{d=n} \cdot 1_{P \equiv A \text{ mod } R_\ell},$$

$$S_{\Lambda_q, \ell}(n, A) = \sum_{d|n} \sum_{P \in \mathbb{P}_q, \deg P = d} d \cdot 1_{P^n \equiv A \text{ mod } R_\ell}.$$

Fix $i \mid n$ and a prime $P \in \mathbb{P}_q$ of degree $i$. To establish Lemma A.1, it suffices to show that $P$ contributes the same weight to each side of (A.1). The contribution of $P$ to the left hand side of (A.1) is

$$1_{i=n} \cdot 1_{P \equiv A \text{ mod } R_\ell}. \quad (A.2)$$

The contribution of $P$ to the right hand side is

$$\frac{\sum_{d|n : i \mid \frac{n}{d}} \mu(d) \sum_{B \in \mathcal{M}_q / R_\ell, B^d \equiv A \text{ mod } R_\ell} 1_{P^d \equiv B \text{ mod } R_\ell}}{n},$$

which may be simplified as

$$\frac{i}{n} \sum_{d|n : i \mid \frac{n}{d}} \mu(d) \sum_{B \in \mathcal{M}_q / R_\ell, B^d \equiv A \text{ mod } R_\ell} 1_{P^d \equiv B \text{ mod } R_\ell} = \frac{i}{n} \sum_{d|\frac{n}{i}} \mu(d) 1_{P^d \equiv A \text{ mod } R_\ell}$$

$$= \frac{i}{n} \cdot 1_{P^i \equiv A \text{ mod } R_\ell} \sum_{d|\frac{n}{i}} \mu(d)$$

$$= \frac{i}{n} \cdot 1_{P^i \equiv A \text{ mod } R_\ell} \cdot 1_{i=n} = 1_{i=n} \cdot 1_{P \equiv A \text{ mod } R_\ell}. \quad (A.3)$$

Here we have used the property $\sum_{d|m} \mu(d) = 1_{m=1}$ of the Möbius function. The expressions (A.2) and (A.3) coincide, as needed.

Remark A.2. Similarly, it may be shown that

$$S_{\Lambda_q, \ell}(n, A) = \frac{\sum_{d|n} \frac{n}{d} \sum_{B \in \mathcal{M}_q / R_\ell, B^d \equiv A \text{ mod } R_\ell} S_{1_{\mathbb{P}_q}, \ell}(\frac{n}{d}, B)}{n}. \quad \square$$
A.2 Solving equations in $M_q/R_\ell$

In order to make use of Lemma [A.1] we describe the following sets. Given $A \in M_q/R_\ell$ and $d \geq 1$, let

$$S_{A,d,t,q} = \{ B \in M_q/R_\ell : B^d \equiv A \mod R_\ell \}. $$

**Lemma A.3.** Let $q = p^e$ be a prime power. Let $\ell \geq 1$ and $A = (a_1, \ldots, a_t) \in M_q/R_\ell$. Let $d \geq 1$ and write it as $d = d' \cdot k$ with $d'$ the largest power of $p$ dividing $d$. Let $e$ be the smallest non-negative integer such that $q^e \geq d'$. If $a_i \not\equiv 0$ for some $d' \parallel i$, then $S_{A,d,t,q} = \emptyset$. Otherwise,

$$S_{A,d,t,q} = \{ (b_1, \ldots, b_t) \in M_q/R_\ell \mid \forall 1 \leq j \leq \left\lfloor \frac{\ell}{d'} \right\rfloor : b_j = \sum_{\sum_i c_i = j} \prod_{c_i = 1} \frac{1}{d'} \left( \sum_{c_i} a_i^{q^e} \right) (c_1, c_2, \ldots, c_t) \}. $$

(A.4)

**Proof.** Let $B = (b_1, \ldots, b_t) \in M_q/R_\ell$. The equation $B^d \equiv A \mod R_\ell$ may be written as

$$ (B^d)^k \equiv A \mod R_\ell. $$

(A.5)

By Lemma [2.3] the exponent of $M_q/R_\ell$ is $p^e$ where $c_1$ is the smallest integer satisfying $p^{c_1} \geq \ell + 1$. Hence we have $g^j \equiv g \mod R_\ell$ whenever $j \equiv 1 \mod p^{c_1}$. In particular, by Euler’s theorem, $g^{k \phi(p^{c_1})} \equiv 1 \mod R_\ell$.

By raising both sides of (A.5) to the $k\phi(p^{c_1})$-th power, we find that (A.5) is equivalent to

$$ B^{d'} \equiv A^{k \phi(p^{c_1})} \mod R_\ell. $$

(A.6)

As we are in characteristic $p$, $(\sum a_i T_i)^{d'} = \sum a_i^{d'} T_i^{d'}$. In particular, the $j$-th coordinate of $B^{d'}$ is 0 if $d' \parallel j$, and is $b_j^{d'}$ otherwise. Since $k \phi(p^{c_1})$ is coprime to the order of the group $M_q/R_\ell$, it follows that $A$ is a $d'$-th power if and only if $A^{k \phi(p^{c_1})}$ is a $d'$-th power. Hence, if $a_j \not\equiv 0$ for some $j$ not divisible by $d'$, then (A.6) is not solvable in $B$. From now on we assume that $a_j = 0$ for any $j$ not divisible by $d'$, and define

$$ \tilde{A} = (a_1^{q^e/d'}, a_2^{q^e/d'}, \ldots, a_t^{q^e/d'}, 0, \ldots, 0) \in M_q/R_\ell, $$

which satisfies $\tilde{A}^d = A$. We define the following truncations of $\tilde{A}$ and $B$:

$$ \tilde{A}_{\text{trunc}} = (a_1^{q^e/d'}, a_2^{q^e/d'}, \ldots, a_t^{q^e/d'}, 0, \ldots, 0) \in M_q/R_{\left[ \frac{1}{d'} \right]}, \quad B_{\text{trunc}} = (b_1, b_2, \ldots, b_{\left[ \frac{1}{d'} \right]}) \in M_q/R_{\left[ \frac{1}{d'} \right]}.$$

Equation (A.6) is equivalent to

$$ B_{\text{trunc}} \equiv \tilde{A}_{\text{trunc}}^{k \phi(p^{c_1})} \mod R_{\left[ \frac{1}{d'} \right]}.$$  

(A.7)

Equation (A.7) is the same as saying that $b_1, \ldots, b_{\left[ \frac{1}{d'} \right]}$ assume the following values:

$$ b_j = \sum_{\sum_i c_i = j} \prod_{c_i = 1} \frac{1}{d'} \left( \sum_{c_i} a_i^{q^e} \right) (c_1, c_2, \ldots, c_{\left[ \frac{1}{d'} \right]}) \in \mathbb{F}_q. $$

(A.8)

To establish (A.4) from (A.3), it remains to show that $(\frac{1}{d'} \sum_{c_i} c_i)$ in (A.8) may be replaced with $(\frac{1}{d'} \sum_{c_i} c_i)$. This follows from Lucas’ Theorem on the values of binomial coefficients modulo primes [Luc78], which tells us that the function

$$ f : \mathbb{Q} \cap \mathbb{Z}_p \to \mathbb{F}_q, \quad x \mapsto \left( \sum c_i \right) $$

depends only on the first $c_3$ $p$-adic digits of its input, where $c_3$ is the smallest integer satisfying $p^{c_3} \geq \sum c_i$. As $\sum c_i \leq \ell$, we have $c_1 \geq c_3$ and Euler’s theorem implies that $k \phi(p^{c_1}) \equiv \frac{1}{k} \mod p^{c_3}$. Thus, $(\frac{1}{d'} \sum_{c_i} c_i) \equiv (\frac{1}{d'} \sum_{c_i} c_i) \mod p$ as needed.

From Lemmas [A.1] and [A.3] we immediately obtain the following proposition.
Proposition A.4. Let \( n, \ell \) be positive integers. Let \( \mathbb{F}_q \) be a finite field of characteristic \( p \). Let \( t_1, \ldots, t_{\ell} \in \mathbb{F}_q \). For any divisor \( d \) of \( n \) not divisible by \( p \), define

\[
\forall 1 \leq j \leq \ell : t_{j,d} = \sum_{i=1}^{\ell} \prod_{i'=1, i' \neq i}^{\ell} t_{i',d} \left( \frac{n}{d} \sum_{c_i} c_i \right) \left( \sum_{c_i} c_i \right) \in \mathbb{F}_q.
\]

For any divisor \( d \) of \( n \) divisible by \( p \) exactly once, define

\[
\forall 1 \leq j \leq \lfloor \frac{\ell}{p} \rfloor : \tilde{t}_{j,d} = \sum_{i=1}^{\lfloor \frac{\ell}{p} \rfloor} \prod_{i'=1, i' \neq i}^{\lfloor \frac{\ell}{p} \rfloor} t_{i',p} \left( \frac{n}{d} \sum_{c_i} c_i \right) \left( \sum_{c_i} c_i \right) \in \mathbb{F}_q. \tag{A.9}
\]

Then we have

\[
\pi_q(n, t_1, \ldots, t_{\ell}) = \frac{1}{n} \sum_{d : p \nmid d | n} \mu(d) \psi_q(n, t_1, t_2, \ldots, t_{\ell}, d) + 1 \psi_{s \leq \ell} s.t. \ p | t_s \cdot \sum_{d : p \nmid d | n, p^2 | d} \mu(d) \psi_q(n, t_1, t_2, \ldots, \tilde{t}_{1, \lfloor \frac{\ell}{p} \rfloor}). \tag{A.10}
\]

A.3 The case \( \ell = 3 \)

Corollary A.5. Let \( q = p^r \) be a prime power and let \( n \in \mathbb{N}_{>0} \). Let \( t_1, t_2, t_3 \in \mathbb{F}_q \).

1. If \( p \geq 5 \) then

\[
\pi_q(n, t_1, t_2, t_3) = \sum_{d : \text{p} b | d | n} \mu(d) \psi_q(n, t_1, t_2, t_3) + 1 \sum_{d : \text{p} b | d | n} \mu(d) \psi_q(n, t_1, t_2, t_3).
\]

2. If \( p = 3 \) then

\[
\pi_q(n, t_1, t_2, t_3) = \sum_{d : 3 \mid d | n} \mu(d) \psi_q(n, t_1, t_2, t_3) + 1 \sum_{d : 3 \mid d | n} \mu(d) \psi_q(n, t_1, t_2, t_3).
\]

3. If \( p = 2 \) then

\[
\pi_q(n, t_1, t_2, t_3) = \sum_{d : 1 \mod 4 | d | n} \mu(d) \psi_q(n, t_1, t_2, t_3) + \sum_{d : 3 \mod 4 | d | n} \mu(d) \psi_q(n, t_1, t_2, t_3) + 1 \sum_{d : 2 | d | n} \mu(d) \psi_q(n, t_1, t_2, t_3).
\]

Proof. Let \( (t_1, t_2, t_3) \in \mathcal{M}_q / R_3 \). Specializing (A.10) to \( \ell = 3 \), we get

\[
\pi_q(n, t_1, t_2, t_3) = \frac{1}{n} \sum_{d : p \nmid d | n} \mu(d) \psi_q(n, t_1, t_2, t_3) + 1 \psi_{s \leq 3} s.t. \ p | t_s \cdot \sum_{d : p \nmid d | n, p^2 | d} \mu(d) \psi_q(n, t_1, t_2, t_3), \tag{A.11}
\]

where \( \tilde{t}_{1, \lfloor \frac{\ell}{p} \rfloor} \) are defined in (A.9).
1. Assume that \( p \geq 5 \). Then the condition that \( t_i = 0 \) if \( i \leq 3 \) and \( p \nmid i \) (appearing in the second term of (A.11)) is equivalent to \( t_1 = t_2 = t_3 = 0 \). This shows that the second term in (A.11) is
\[
1_{t_1=t_2=t_3=0} \cdot \frac{1}{n} \sum_{p \mid d \mid n} \mu(d) \psi_q \left( \frac{n}{d} \right). \tag{A.12}
\]
From (A.11), (A.12) and (1.4), the first case of the corollary is established.

2. Assume that \( p = 3 \). Then the condition that \( t_i = 0 \) if \( i \leq 3 \) and \( 3 \nmid i \) (appearing in the second term of (A.11)) is equivalent to \( t_1 = t_2 = 0 \). This shows that the second term in (A.11) is
\[
1_{t_1=t_2=0} \cdot \frac{1}{n} \sum_{3 \mid d \mid n, 9 \nmid d} \mu(d) \psi_q \left( \frac{n}{d} \right) \frac{1}{d/3} t_1. \tag{A.13}
\]
From (A.11), (A.13) and (3.3), the second case of the corollary is established.

3. Assume that \( p = 2 \). Then the condition that \( t_i = 0 \) if \( i \leq 3 \) and \( 2 \nmid i \) (appearing in the second term of (A.11)) is equivalent to \( t_1 = t_3 = 0 \). This shows that the second term in (A.11) is
\[
1_{t_1=t_3=0} \cdot \frac{1}{n} \sum_{2 \mid d \mid n, 4 \nmid d} \mu(d) \psi_q \left( \frac{n}{d} \right) \frac{1}{d/2} t_2. \tag{A.14}
\]
From (A.11), (A.14) and (3.3), we find that
\[
\pi_q(n, t_1, t_2, t_3) = \frac{1}{n} \sum_{2 \mid d \mid n} \mu(d) \psi_q \left( \frac{n}{d} \right) \frac{t_1}{d} \frac{t_2}{d} + \frac{1-d}{2d^2} t_1^2, \frac{t_2}{d} + \frac{1-d}{2d^2} t_1 t_2 + \frac{(2d-1)(d-1)}{6d^3} t_1^3 + 1_{t_1=t_3=0} \cdot \frac{1}{n} \sum_{2 \mid d \mid n} \mu(d) q^{\frac{n}{d} - 1}. \tag{A.15}
\]
If \( 2 \nmid d \mid n \), then we have the following equalities in \( \mathbb{F}_q \):
\[
\frac{t_2}{d} + \frac{1-d}{2d^2} t_1^2 = \begin{cases} t_2 & \text{if } d \equiv 1 \mod 4, \\ t_2 + t_1^2 & \text{if } d \equiv 3 \mod 4, \end{cases} \tag{A.16}
\]
\[
\frac{t_3}{d} + \frac{1-d}{d^2} t_1 t_2 + \frac{(2d-1)(d-1)}{6d^3} t_1^3 = \begin{cases} t_3 & \text{if } d \equiv 1 \mod 4, \\ t_3 + t_1^3 & \text{if } d \equiv 3 \mod 4. \end{cases}
\]
The third case of the corollary follows from (A.15) and (A.16).

\[
\square
\]

References

[AGG+16] Omran Ahmadi, Furuk Göloğlu, Robert Granger, Gary McGuire, and Emrah Serican Yilmaz. Fibre products of supersingular curves and the enumeration of irreducible polynomials with prescribed coefficients. *Finite Fields and Their Applications*, 42:128–164, 2016.

[BBSR15] Efrat Bank, Lior Bary-Soroker, and Lior Rosenzweig. Prime polynomials in short intervals and in arithmetic progressions. *Duke Mathematical Journal*, 164(2):277–295, 2015.

[Car38] Leonard Carlitz. A class of polynomials. *Trans. Amer. Math. Soc.*, 43(2):167–182, 1938.

[Car52] L Carlitz. A theorem of Dickson on irreducible polynomials. *Proceedings of the American Mathematical Society*, 3(5):693–700, 1952.

[CMR+03] K Cattell, CR Miers, F Ruskey, J Sawada, and M Serra. The number of irreducible polynomials over \( \text{GF}(2) \) with given trace and subtrace. *Journal of Combinatorial Mathematics and Combinatorial Computing*, 47:31–64, 2003.
[Coh72] Stephen D Cohen. Uniform distribution of polynomials over finite fields. *J. London Math. Soc.*, 6(2):93–102, 1972.

[DE01] Persi Diaconis and Steven N. Evans. Linear functionals of eigenvalues of random matrices. *Trans. Amer. Math. Soc.*, 353(7):2615–2633, 2001.

[Dic58] Leonard Eugene Dickson. *Linear groups: With an exposition of the Galois field theory*. with an introduction by W. Magnus. Dover Publications, Inc., New York, 1958.

[EH91] Gove W Effinger and David R Hayes. *Additive number theory of polynomials over a finite field*. Oxford University Press, USA, 1991.

[Fom96] MN Fomenko. Some L-functions of a polynomial ring over a finite field. *Algebra and Logic*, 35(4):266–278, 1996.

[FY03] Robert W Fitzgerald and Joseph I. Yucas. Irreducible polynomials over GF(2) with three prescribed coefficients. *Finite Fields and Their Applications*, 9(3):286–299, 2003.

[Gau65] Carl Friedrich Gauss. *Arithmetische untersuchungen*. Chelsea, 1965.

[Gra95] Andrew Granville. Unexpected irregularities in the distribution of prime numbers. In *Proceedings of the International Congress of Mathematicians, Vol. 1, 2 (Zürich, 1994)*, pages 388–399. Birkhäuser, Basel, 1995.

[Hay65] David R Hayes. The distribution of irreducibles in GF[q, x]. *Transactions of the American Mathematical Society*, 117:101–127, 1965.

[Hay74] D. R. Hayes. Explicit class field theory for rational function fields. *Trans. Amer. Math. Soc.*, 189:77–91, 1974.

[HB88] D. R. Heath-Brown. The number of primes in a short interval. *J. Reine Angew. Math.*, 389:22–63, 1988.

[Hsu96] Chih-Nung Hsu. The distribution of irreducible polynomials in $F_q[t]$. *Journal of Number Theory*, 61(1):85–96, 1996.

[Hux72] M. N. Huxley. On the difference between consecutive primes. *Invent. Math.*, 15:164–170, 1972.

[IR90] Kenneth Ireland and Michael Rosen. *A classical introduction to modern number theory*, volume 84 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1990.

[Kat05] Nicholas M. Katz. *Moments, monodromy, and perversity: a Diophantine perspective*, volume 159 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 2005.

[Kat13] Nicholas M Katz. Witt vectors and a question of Keating and Rudnick. *International Mathematics Research Notices*, 2013(16):3613–3638, 2013.

[KR14] Jonathan P Keating and Zeév Rudnick. The variance of the number of prime polynomials in short intervals and in residue classes. *International Mathematics Research Notices*, 2014(1):259–298, 2014.

[Kro57] Leopold Kronecker. Zwei sätze über gleichungen mit ganzzahligen coefficienten. *Journal für die reine und angewandte Mathematik*, 53:173–175, 1857.

[Kuz89] EN Kuz’min. Irreducible polynomials over a finite field. *Siberian Mathematical Journal*, 30(6):915–925, 1989.

[Kuz91] EN Kuz’min. Irreducible polynomials over a finite field and an analogue of Gauss sums over a field of characteristic 2. *Siberian Mathematical Journal*, 32(6):982–989, 1991.

[Kuz94] EN Kuz’min. Irreducible polynomials over finite fields. i. *Algebra and Logic*, 33(4):216–232, 1994.
Matilde Lalín and Olivier Larocque. The number of irreducible polynomials with the first two prescribed coefficients over a finite field. *Rocky Mountain J. Math.*, 46(5):1587–1618, 2016.

Édouard Lucas. Sur les congruences des nombres eulériens et des coefficients différentiels des fonctions trigonométriques suivant un module premier. *Bulletin de la Société mathématique de France*, 6:49–54, 1878.

Marko Moisio and Kalle Ranto. Elliptic curves and explicit enumeration of irreducible polynomials with two coefficients prescribed. *Finite Fields and Their Applications*, 14(3):798–815, 2008.

Georges Rhin. Répartition modulo 1 dans un corps de séries formelles sur un corps fini. *Dissertationes Math. (Rozprawy Mat.)*, 95, 1972.

Won-Ho Ri, Gum-Chol Myong, Ryul Kim, and Chang-Il Rim. The number of irreducible polynomials over finite fields of characteristic 2 with given trace and subtrace. *Finite Fields and Their Applications*, 29:118–131, 2014.

Frank Ruskey, C Robert Miers, and Joe Sawada. The number of irreducible polynomials and Lyndon words with given trace. *SIAM Journal on Discrete Mathematics*, 14(2):240–245, 2001.

Michael Rosen. *Number Theory in Function Fields*, volume 210. Springer Science & Business Media, 2002.

Gerard Van der Geer and Marcel Van der Vlugt. Reed-Muller codes and supersingular curves. i. *Compositio Mathematica*, 84(3):333–367, 1992.

Helge von Koch. Sur la distribution des nombres premiers. *Acta Math.*, 24(1):159–182, 1901.

André Weil. *Basic Number Theory*. Springer Nature, 1974.

Kenneth S Williams. Note on cubics over GF(2^n) and GF(3^n). *Journal of Number Theory*, 7(4):361–365, 1975.

Joseph L Yucas and Gary L Mullen. Irreducible polynomials over GF(2) with prescribed coefficients. *Discrete Mathematics*, 274(1):265–279, 2004.

Joseph L Yucas. Irreducible polynomials over finite fields with prescribed trace/prescribed constant term. *Finite Fields and Their Applications*, 12(2):211–221, 2006.

Raymond and Beverly Sackler School of Mathematical Sciences, Tel Aviv University, Tel Aviv 69978, Israel. E-mail address: ofir.goro@gmail.com