PRIME POWER EXPONENTIAL AND CHARACTER SUMS WITH EXPLICIT EVALUATIONS

by

VINCENT PIGNO

B.S., University of Kansas, 2008

M.S., Kansas State University, 2012

AN ABSTRACT OF A DISSERTATION

submitted in partial fulfillment of the
requirements for the degree

DOCTOR OF PHILOSOPHY

Department of Mathematics
College of Arts and Sciences

KANSAS STATE UNIVERSITY
Manhattan, Kansas

2014

Abstract

Exponential and character sums occur frequently in number theory. In most applications one is only interested in estimating such sums. Explicit evaluations of such sums are rare. In this thesis we succeed in evaluating three types of mod p^m sums when p is a prime and m is sufficiently large. The twisted monomial sum,

$$S_1 = \sum_{x=1}^{p^m} \chi(x) e^{2\pi i n x^k / p^m},$$

the binomial character sum,

$$S_2 = \sum_{x=1}^{p^m} \chi_1(x)\chi_2(Ax^k + B),$$

and the generalized Jacobi sum,

$$S_3 = J_{p^n}(\chi_1, \ldots, \chi_k, p^m) = \sum_{x_1=1}^{p^m} \cdots \sum_{\substack{x_k=1 \\ x_1+\cdots+x_k=p^n}}^{p^m} \chi_1(x_1)\cdots\chi_k(x_k), \quad m > n,$$

where the χ are mod p^m Dirichlet characters.

We additionally show that these are all sums which can be expressed in terms of classical Gauss sums.

PRIME POWER EXPONENTIAL AND CHARACTER SUMS WITH EXPLICIT EVALUATIONS

by

Vincent Pigno

B.S., University of Kansas, 2008

M.S., Kansas State University, 2012

A DISSERTATION

submitted in partial fulfillment of the
requirements for the degree

DOCTOR OF PHILOSOPHY

Department of Mathematics
College of Arts and Sciences

KANSAS STATE UNIVERSITY
Manhattan, Kansas

2014

Approved by:

Major Professor
Christopher Pinner

Abstract

Exponential and character sums occur frequently in number theory. In most applications one is only interested in estimating such sums. Explicit evaluations of such sums are rare. In this thesis we succeed in evaluating three types of mod p^m sums when p is a prime and m is sufficiently large. The twisted monomial sum,

$$S_1 = \sum_{x=1}^{p^m} \chi(x) e^{2\pi i n x^k / p^m},$$

the binomial character sum,

$$S_2 = \sum_{x=1}^{p^m} \chi_1(x)\chi_2(Ax^k + B),$$

and the generalized Jacobi sum,

$$S_3 = J_{p^n}(\chi_1, \ldots, \chi_k, p^m) = \sum_{x_1=1}^{p^m} \cdots \sum_{\substack{x_k=1 \\ x_1+\cdots+x_k=p^n}}^{p^m} \chi_1(x_1)\cdots\chi_k(x_k), \quad m > n,$$

where the χ are mod p^m Dirichlet characters.

We additionally show that these are all sums which can be expressed in terms of classical Gauss sums.

Table of Contents

Acknowledgments

The entirety of thesis represents joint work with my friend and advisor Professor Chris Pinner. Additionally Chapter 6 is joint work with Joe Sheppard, Chapter 7 is joint work with Misty Long and Chapter 3 contains joint work with both Joe and Misty.

I would like to express my gratitude to my wife and family for supporting me through the completion of this thesis.

Additionally I would like to thank the entire faculty and staff of the Kansas State University Department of Mathematics. I could not have asked for better role models and mentors. Specifically, the Number Theory group: Professor Todd Cochrane, Professor Craig Spencer, and Chris Pinner. Thanks as well to Professors Virgina Naibo, Andrew Bennett, Andy Chermak, Bob Burckel, Marianne Korten, Dr. Worm, and Gown Swift.

A special thank you is deserved by Reta McDermott and Kathy Roeser for all their assistance and patience.

I would also like to thank the additional members of my committee, Professor Gary Gadbury and Professor Mitchell Neilsen for their comments and time.

A big shout out to Buggin' Out Crew, for continually pushing me to work hard and think creatively.

Dedication

This thesis is dedicated to my uncle, Francis Pigno.

Chapter 1

Introduction

We are concerned here with the explicit evaluations of certain exponential sums modulo p^m where p is a prime, namely the twisted monomial sum,

$$S_1 = S_1(\chi, nx^k, p^m) = \sum_{x=1}^{p^m} \chi(x) e_{p^m}(nx^k), \tag{1.1}$$

where

$$e_q(x) := e^{2\pi i x/q}, \tag{1.2}$$

the binomial character sum,

$$S_2 = S_2(\chi_1, \chi_2, Ax^k + B, p^m) = \sum_{x=1}^{p^m} \chi_1(x)\chi_2(Ax^k + B), \tag{1.3}$$

and the generalized Jacobi sum,

$$S_3 = J_{p^n}(\chi_1, \ldots, \chi_k, p^m) = \sum_{x_1=1}^{p^m} \cdots \sum_{\substack{x_k=1 \\ x_1+\cdots+x_k=p^n}}^{p^m} \chi_1(x_1)\cdots\chi_k(x_k), \quad m > n, \tag{1.4}$$

where the χ are multiplicative characters. We will show all of these sums can be explicitly evaluated when m is sufficiently large. Cases where exponential sums can be evaluated are rare, making the sums which can be specifically evaluated standouts. As we shall see in Chapter 4 these are all sums which can be expressed in terms of classical Gauss sums.

In order to obtain our evaluations we apply the reduction method of T. Cochrane and Z. Zheng [4], thereby reducing our sums to the consideration of a particular characteristic equation. In Chapter 5 we reduce the twisted monomial sum,

$$S_1 = \sum_{x=1}^{p^m} \chi(x) e_{p^m}\left(nx^{\gamma p^t}\right),$$

with $p \nmid \gamma$, to the equation

$$c_1 + R_{t+1} n x^{\gamma p^t} \equiv 0 \mod p^{m-t-1} \tag{1.5}$$

when $t+1 < m < 2t+2$, and to

$$c_1 + R_{t+s+1} n x^{\gamma p^t} \equiv 0 \mod p^{t+s+1}, \tag{1.6}$$

when $2t+2 \leq m$, where the R_j are parameters dependent on our choice of a primitive root mod p^m and the c_i's are parameters depending on the character (these parameters will be discussed in detail in Chapter 2). Depending on the range, if (1.5) or (1.6) has no solution the sum is zero; however if there is a solution we are able to directly evaluate the sum as shown in the following theorem, which appears as Theorem 5.1.1 in Chapter 5.

Theorem 1.0.1. *For p an odd prime, $t \in \mathbb{Z}$, $t \geq 0$, let*

$$f(x) = nx^{\gamma p^t}, \quad p \nmid n\gamma.$$

Case I: Suppose that $t+1 < m \leq 2t+2$. If χ is a dp^t-th power of a primitive character

and the characteristic equation (1.5) *has a solution* α *then*

$$S_1(\chi, f(x), p^m) = dp^{m-1}\chi(\alpha)e_{p^m}(f(\alpha)).$$

Otherwise, $S(\chi, f(x), p^m) = 0$.

Case II: Suppose that $2t + 2 < m$. *If* χ *is a* dp^t*-th power power of a primitive character and* (1.6) *has a solution then*

$$S_1(\chi, f(x), p^m) = dp^{\frac{m}{2}+t}\chi(\alpha)e_{p^m}(f(\alpha))\left(\frac{-2rc_1}{p^m}\right)\varepsilon_{p^m}, \tag{1.7}$$

where α *is a solution of* (1.6), $\left(\frac{\cdot}{p^m}\right)$ *is the Jacobi symbol,* ε_{p^m} *is as in* (2.29) *and* $d = (\gamma, p-1)$.

It should be pointed out that in absolute value this result simplifies to $S_1 = 0$ or

$$|S_1(\chi, f(x), p^m)| = \begin{cases} dp^{m-1}, & \text{if } t+1 < m \leq 2t+2, \\ dp^{\frac{m}{2}+t}, & \text{if } 2t+2 < m. \end{cases}$$

We get a similar evaluation when $p = 2$, dependent again on solutions to certain characteristic equations.

In Chapter 6 we evaluate the pure character sum,

$$S_2 = \sum_{x=1}^{p^m} \chi_1(x)\chi_2(Ax^k + B).$$

Again using the methods of Cochrane and Zheng we obtain a characteristic equation,

$$g'(x) \equiv 0 \bmod p^{\min\left\{m-1, [\frac{m+n}{2}]+t\right\}} \tag{1.8}$$

where $g'(x)$ comes from writing $\chi_1(x)\chi_2(Ax^k + B) = \chi(g(x))$ for some mod p^m character χ,

leading to the following evaluation; see Theorem 6.1.1.

Theorem 1.0.2. *Suppose that p is an odd prime and χ_1, χ_2 are mod p^m characters with χ_2 primitive.*

If $\chi_1 = \chi_3^k$, and (1.8) has a solution x_0 with $p \nmid x_0(Ax_0^k + B)$, then

$$\sum_{x=1}^{p^m} \chi_1(x)\chi_2(Ax^k + B) = d\chi_1(x_0)\chi_2(Ax_0^k + B) \begin{cases} p^{m-1}, & \text{if } t+n+1 < m \le 2t+n+2, \\ p^{\frac{m+n}{2}+t}, & \text{if } m > 2t+n+2,\ m-n \text{ even}, \\ p^{\frac{m+n}{2}+t}\varepsilon_1, & \text{if } m > 2t+n+2,\ m-n \text{ odd}, \end{cases}$$

where ε_1 is as in (6.13)

If χ_1 does not satisfy $\chi_1 = \chi_3^k$, or (1.8) has no solution satisfying $p \nmid x_0(Ax_0^k + B)$, then the sum is zero.

For $p = 2$ similar results are obtained in Chapter 6; see Theorem 6.2.1.

In order to evaluate the multi-variable general Jacobi sum, (1.4), we use a general result from Chapter 4, that expresses S_1, S_2 and S_3 in terms of the classical Gauss sum,

$$G(\chi, p^m) = \sum_{x=1}^{p^m} \chi(x) e_{p^m}(x).$$

For example, when the characters are primitive,

$$J_{p^n}(\chi_1, \dots, \chi_k, p^m) = \frac{\prod_{i=1}^k G(\chi_i, p^m)}{G(\chi_1 \dots \chi_k, p^{m-n})}. \tag{1.9}$$

In Chapter 3 we use the Cochrane and Zheng reduction method to get the following evaluation of the mod p^m Gauss sum; see Theorem 3.1.

Theorem 1.0.3. *Suppose that χ is a mod p^m character with $m \ge 2$. If χ is imprimitive,*

then $G(\chi, p^m) = 0$. *If* χ *is primitive, then*

$$G(\chi, p^m) = p^{\frac{m}{2}} \chi\left(-cR_j^{-1}\right) e_{p^m}\left(-cR_j^{-1}\right) \begin{cases} \left(\frac{-2rc}{p}\right)^m \varepsilon_{p^m}^m, & \text{if } p \neq 2, \text{ and } p^m \neq 3^3, \\ \left(\frac{2}{c}\right)^m \omega^c, & \text{if } p = 2 \text{ and } m \geq 5, \end{cases} \tag{1.10}$$

for any $j \geq \lceil \frac{m}{2} \rceil$ *when* p *is odd and any* $j \geq \lceil \frac{m}{2} \rceil + 2$ *when* $p = 2$. *Here* x^{-1} *denotes the inverse of* x *mod* p^m, *and* $\omega := e^{\pi i/4}$.

Using (1.9) and Theorem 1.0.3 we are then able to evaluate S_3 explicitly; see Theorem 7.0.1 (we write all three of our sums in terms of Gauss sums in Chapter 4, however we only use this for direct evaluation in the case of our multi-variable Jacobi sum).

Theorem 1.0.4. *Let* p *be a prime and* $m \geq n + 2$. *Suppose that* $\chi_1, \ldots, \chi_k$ *are* $k \geq 2$ *characters mod* p^m *with at least one of them primitive.*

If the $\chi_1, \ldots, \chi_k$ *are not all primitive mod* p^m *or* $\chi_1 \ldots \chi_k$ *is not induced by a primitive mod* p^{m-n} *character, then* $J(\chi_1, \ldots, \chi_k, p^m) = 0$.

If the $\chi_1, \ldots, \chi_k$ *are primitive mod* p^m *and* $\chi_1 \cdots \chi_k$ *is primitive mod* p^{m-n}, *then*

$$J_{p^n}(\chi_1, \ldots, \chi_k, p^m) = p^{\frac{1}{2}(m(k-1)+n)} \frac{\chi_1(c_1) \cdots \chi_k(c_k)}{\chi_1 \cdots \chi_k(v)} \delta, \tag{1.11}$$

for p *odd,*

$$\delta = \left(\frac{-2r}{p}\right)^{m(k-1)+n} \left(\frac{v}{p}\right)^{m-n} \left(\frac{c_1 \cdots c_k}{p}\right)^m \varepsilon_{p^m}^k \varepsilon_{p^{m-n}}^{-1},$$

and

$$v := p^{-n}(c_1 + \cdots + c_k), \quad \omega := e^{\pi i/4}. \tag{1.12}$$

Evaluations of 1.4 are also given when $p = 2$ in Chapter 7; see Theorem 7.0.1.

Chapter 2

Preliminaries

Let q be a positive integer. For a multiplicative Dirichlet character χ mod q and $f(x), g(x) \in \mathbb{Z}[x]$ we define a mixed exponential sum

$$S(\chi, g(x), f(x), q) := \sum_{x=1}^{q} \chi(g(x)) e_q(f(x)) \tag{2.1}$$

where

$$e_q(x) = e^{2\pi i x/q}. \tag{2.2}$$

Note it is sometimes useful to use the equivalent notation

$$e\left(\frac{x}{q}\right) = e^{2\pi i x/q}. \tag{2.3}$$

We are concerned here with the explicit evaluations of these and closely related sums when $q = p^m$ with p a prime and f, g are specific polynomials with integer coefficients, namely (1.1), (1.3) and (1.4). We show in Section 2.2 why it is enough to reduce to the prime power case, but we first start with some definitions and preliminaries.

2.1 Dirichlet Characters

We begin by defining a special class of multiplicative homomorphisms called group characters.

Definition 2.1.1. *Given a finite group $\langle G, * \rangle$ a character χ is a function $\chi : G \to \mathbb{C}^*$ such that for $a, b \in G$, $\chi(a * b) = \chi(a)\chi(b)$.*

For the identity element, e, and some a in G we have $\chi(a) = \chi(e * a) = \chi(e)\chi(a)$ and since χ is nonzero on G, we have $\chi(e) = 1$. Further, $\chi(a)^{|G|} = \chi(e) = 1$, and thus $\chi(a)$ is a $|G|$-th root of unity.

For any finite abelian group, G, we know that $G \cong \mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_r}$ where the $\mathbb{Z}_{n_i}$ are additive cyclic groups. Let the generators of G be $a_1 = (1, 0, \ldots, 0)$, $\ldots$, $a_r = (0, \ldots, 0, 1)$. For a generator a_i we have that $\chi(a_i)^{n_i} = \chi(n_i a_i) = \chi(0) = 1$; thus $\chi(a_i)$ is an n_ith root of unity. Since we know $\chi(a_i) = e_{n_i}(c_i)$ for some integer $0 \leq c_i \leq n_i - 1$ we have exactly n_i distinct places to send each a_i resulting in $\prod_{i=1}^{r} n_i = |G|$ different characters. We also note that for finitely generated groups the characters are defined by their actions on the generators.

In this thesis we let $G = \mathbb{Z}_q^*$ where we write $\mathbb{Z}_q^*$ for the multiplicative group of units in $\mathbb{Z}/q\mathbb{Z}$. The characters on $\mathbb{Z}_q^*$ are then extended to all of $\mathbb{Z}_q$ by defining the characters to be zero on elements of $\mathbb{Z}_q$ not in $\mathbb{Z}_q^*$.

Definition 2.1.2. *A Dirichlet character χ mod q is a non-identically zero function $\chi : \mathbb{Z}_q \to \mathbb{C}$ with $\chi(ab) = \chi(a)\chi(b)$ for all $a, b \in \mathbb{Z}_q$ and $\chi(c) = 0$ if $(q, c) > 1$.*

One of the most well known examples of a Dirichlet character is the Legendre symbol. We define the Legendre symbol modulo a prime, p, by

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{if } (a,p) = 1, \text{ and a is a square mod } p, \\ -1, & \text{if } (a,p) = 1, \text{ and a is not a square mod } p, \\ 0, & \text{if } (a,p) > 1. \end{cases} \tag{2.4}$$

Alternately we will denote the Legendre symbol as the quadratic character χ_Q.

For $q_1 \mid q$ we say that a mod q character χ is *induced* by a mod q_1 character, χ_{q_1}, if

$$\chi(n) = \begin{cases} \chi_{q_1}(n), & \text{if } (n,q) = 1, \\ 0, & \text{otherwise.} \end{cases}$$

We call a character primitive if it cannot be induced by a lower modulus character.

One can examine the structure Dirichlet characters by examining the characters on prime powers. Letting the prime factorization of $q = \prod_{i=1}^{k} p_i^{\alpha_i}$ where p_i are primes, we claim that there exists a corresponding primitive root a_i such that $\mathbb{Z}^*_{p_i^{\alpha_i}} = \langle a_i \rangle$ unless $p_i = 2$, with $\alpha_i \geq 3$ in which case $\mathbb{Z}^*_{2^{\alpha_i}} = \langle -1, 5 \rangle$ (see Section 2.8 in [18]). The order of each a_i mod $p_i^{\alpha_i}$ is exactly $\phi(p_i^{\alpha_i})$, and thus $\chi(a_i)$ is a $\phi(p_i^{\alpha_i})$ root of unity unless $p_i = 2$ with $\alpha_i \geq 3$ in which case 5 has order $2^{\alpha-2}$ and -1 has order 2 and thus $\chi(-1)$ is a 2-nd root of unity and $\chi(5)$ is a 2^{α_i-2}-nd root of unity. The characters of $\mathbb{Z}^*_{p_i^{\alpha_i}}$ are defined by their action on the a_i's, that is

$$\chi(a_i) = e_{\phi(p_i^{\alpha_i})}(c_i), \quad 1 \leq c_i \leq \phi(p_i^{\alpha_i}) \tag{2.5}$$

unless $p_i = 2$ with $\alpha_i \geq 3$ when we have

$$\chi(-1) = \pm 1, \quad \chi(5) = e_{2^{\alpha_i-2}}(c_i), \quad 1 \leq c_i \leq \phi(2^{\alpha_i-2}). \tag{2.6}$$

For any mod $p_i^{\alpha_i}$ character χ we can extend χ to be a mod q character by defining it to be 0 for all $a \in \mathbb{Z}_q$ with $(a,q) > 1$. We additionally note that for two mod q characters, χ_1 and χ_2, we have that $\chi_1\chi_2$ is also a mod q character.

We claim that every mod q character can be be written as the product k mod q characters induced by mod $p_i^{\alpha_i}$ characters, $i = 1, \ldots, k$. The number of characters for $\mathbb{Z}^*_{p_i^{\alpha_i}}$ is $\phi(p_i^{\alpha_i})$; thus we have $\prod_{i=1}^{k} \phi(p_i^{\alpha_i}) = \phi(q)$ choices for a mod q character χ of the form $\chi = \chi_1 \ldots \chi_k$ where the χ_i are mod q characters induced by mod $p_i^{\alpha_i}$ characters. As there are $\phi(q)$

characters for $\mathbb{Z}_q^*$ if each of the choices of χ_i gives a different mod q character then every mod q character may be constructed in this way. Let χ' and χ'' be two mod q characters with $\chi' = \chi''$, and $\chi' = \chi'_1 \dots \chi'_k$, $\chi'' = \chi''_1 \dots \chi''_k$, where the χ'_i and χ''_i are induced by mod $p_i^{\alpha_i}$ characters. By the Chinese Remainder Theorem for each a_i there exists an $A_i \equiv a_i \bmod p_i^{\alpha_i}$ with $A_i \equiv 1 \bmod p_j^{\alpha_j}$, for $j \neq i$. When $p_i = 2$ with $\alpha_i \geq 3$ we also need an $A_i \equiv 5 \bmod 2^{\alpha_i}$ and $A_0 \equiv -1 \bmod 2^{\alpha_i}$, $A_i \equiv A_0 \equiv 1 \bmod p^{\alpha_j}$, $i \neq j$. For $2^3 \nmid p_j^{\alpha_j}$, $\chi'(A_j) = \chi''(A_j)$, and thus $\chi'_j(a_j) = \chi''_j(a_j)$. When $p_j = 2$ with $\alpha_j \geq 3$ we have that $\chi'(A_j) = \chi''(A_j)$ and $\chi'(A_0) = \chi''(A_0)$, implying that $\chi'_j(5) = \chi''_j(5)$ and $\chi'_j(-1) = \chi''_j(-1)$. Since a $p_i^{\alpha_i}$ character is determined by it action on the generators of $\mathbb{Z}^*_{p_i^{\alpha_i}}$, χ'_j and χ''_j must be the same character for each j. Therefore, any mod q character, χ can be expressed as

$$\chi = \chi_1 \dots \chi_k \tag{2.7}$$

where the χ_i are mod q characters induced by mod $p_i^{\alpha_i}$ characters.

The character which sends all the elements of the multiplicative group to 1 is called the principal character, defined by

$$\chi_0(b) = \begin{cases} 1, & \text{if } (q,b) = 1, \\ 0 & \text{else.} \end{cases}$$

2.2 Reducing to the case of prime modulus

Let $q = \prod_{x=1}^{k} p_i^{\alpha_i}$ with p_i prime. For a mod q mixed exponential sum we will use the fact that any mod q character, $\chi = \chi_1 \dots \chi_k$, where the χ_i are mod $p_i^{\alpha_i}$ characters extended to $\mathbb{Z}_q$ to break our composite sums up into sums modulo prime powers. Define $m_i = q/p_i^{\alpha_i}$ and let h_i be integers such that $\sum_{j=1}^{k} h_j m_j = 1$. Note that $\sum_{j=1}^{k} x_j h_j m_j \equiv x_i h_i m_i \equiv x_i \bmod p_i^{\alpha_i}$, thus

$$g(x_1 h_1 m_1 + \dots + x_k h_k m_k) \equiv g(x_i) \bmod p_i^{\alpha_i}.$$

Further,

$$(x_1h_1m_1 + \cdots + x_kh_km_k)^j \equiv (x_1h_1m_1)^j + \cdots + (x_kh_km_k)^j \bmod q$$

giving

$$\begin{aligned} e_q\left((x_1h_1m_1 + \cdots + x_kh_km_k)^j\right) &= e_q\left((x_1h_1m_1)^j + \cdots + (x_kh_km_k)^j\right) \\ &= \prod_{i=1}^{k} e_{p_i^{\alpha_i}}(h_i^j m_i^{j-1} x_i^j) = \prod_{i=1}^{k} e_{p_i^{\alpha_i}}(h_i x_i^j). \end{aligned}$$

Thus

$$e_q\left(f(x)\right) = \prod_{i=1}^{k} e_{p_i^{\alpha_i}}(h_i f(x_i)).$$

We may assume that $f(0) = 0$, for if not we may write $e_q(f(x)) = e_q(f(x)-f(0))e_q(f(0))$ and the $e_q(f(0))$ can be pulled out of the sum straightaway. Additionally $x_1h_1m_1 + \cdots + x_kh_km_k$ runs over a complete set of residues modulo q as the x_i's run from $1, \ldots, p_i^{\alpha_i}$. So for the general mod q mixed exponential sum, (2.1), we have

$$\begin{aligned} S(\chi, g(x), f(x), q) &= \sum_{x=1}^{q} \chi(g(x)) e_q(f(x)) \\ &= \sum_{x_1=1}^{p_1^{\alpha_1}} \chi_1(g(x_1)) e_{p_1^{\alpha_1}}(h_1 f(x_1)) \cdots \sum_{x_k=1}^{p_k^{\alpha_k}} \chi_k(g(x_k)) e_{p_k^{\alpha_k}}(h_k f(x_k)) \\ &= \prod_{i=1}^{k} S(\chi_i, g(x), h_i f(x), p_i^{\alpha_i}). \end{aligned}$$

Thus, for the general mixed exponential sum is suffices to deal only with the case $q = p^\alpha$ which includes our S_1, (1.1).

Similarly if χ', and χ'' are mod q characters then our S_2 sum,

$$\begin{aligned} S_2(\chi', \chi'', Ax^k + B, q) &= \sum_{x=1}^{q} \chi'(x)\chi''(Ax^k + B) \\ &= \prod_{i=1}^{k} \sum_{x_i=1}^{p_i^{\alpha_i}} \chi_i'(x_i)\chi_i''(Ax_i^k + B) \\ &= \prod_{i=1}^{k} S_2(\chi_i', \chi_i'', Ax^k + B, p_i^{\alpha_i}), \end{aligned}$$

for χ_i', χ_i'' induced by mod $p_i^{\alpha_i}$ characters. For S_2 it suffices to examine only prime powers.

Likewise, for the generalized Jacobi sum,

$$J_B(\chi_1, \ldots, \chi_k, q) = \sum_{\substack{x_1=1 \\ x_1+\cdots+x_k \equiv B \bmod q}}^{q} \cdots \sum_{x_k=1}^{q} \chi_1(x_1) \cdots \chi_k(x_k),$$

if the χ_i are mod rs characters with $(r, s) = 1$ then, writing $\chi_i = \chi_i'\chi_i''$ where χ_i' and χ_i'' are mod r and mod s characters respectively, writing $x_i = u_i rr^{-1} + v_i ss^{-1}$, where $u_i = 1, \ldots, s$, $v_i = 1, \ldots, r$, and $rr^{-1} + ss^{-1} = 1$, gives

$$\begin{aligned} J_B(\chi_1, \ldots, \chi_k, rs) &= \sum_{\substack{u_1=1 \\ (rr^{-1}u_1+ss^{-1}v_1)+\cdots+(rr^{-1}u_k+ss^{-1}v_k) \equiv B \bmod rs}}^{s} \sum_{v_1=1}^{r} \cdots \sum_{u_k=1}^{s} \sum_{v_k=1}^{r} \chi_1(rr^{-1}u_1 + ss^{-1}v_1) \cdots \chi_k(rr^{-1}u_k + ss^{-1}v_k), \\ &= \sum_{\substack{u_1=1 \\ (rr^{-1}u_1+ss^{-1}v_1)+\cdots+(rr^{-1}u_k+ss^{-1}v_k) \equiv B \bmod s \\ (rr^{-1}u_1+ss^{-1}v_1)+\cdots+(rr^{-1}u_k+ss^{-1}v_k) \equiv B \bmod r}}^{s} \sum_{v_1=1}^{r} \cdots \sum_{u_k=1}^{s} \sum_{v_k=1}^{r} \chi_1''(rr^{-1}u_1)\chi_1'(ss^{-1}v_1) \ldots \chi_k''(rr^{-1}u_k)\chi_k'(ss^{-1}v_k) \\ &= \sum_{\substack{u_1=1 \\ u_1+\cdots+u_k \equiv B \bmod s}}^{s} \cdots \sum_{u_k=1}^{s} \chi_1''(u_1) \ldots \chi_k''(u_k) \sum_{\substack{v_1=1 \\ v_1+\cdots+v_k \equiv B \bmod r}}^{r} \cdots \sum_{v_k=1}^{r} \chi_1'(v_1) \ldots \chi_k'(v_k). \\ &= J_B(\chi_1', \ldots, \chi_k', r) J_B(\chi_1'', \ldots, \chi_k'', s). \end{aligned}$$

Hence, it suffices to consider the case of prime power moduli, $q = p^m$, for all three of our sums.

2.3 The Power-Full Lemma

A most useful result for manipulating mixed and pure exponential sums is the connection between the degree of the polynomials f, g and the type of character necessary for the sum to not be zero. For instance in order to write our sums (1.1), (1.3) and (1.4) in terms of Gauss sums (which will be discussed in Chapter 4) we must first prove the following powerful lemma

Lemma 2.3.1. *For any odd prime p, multiplicative characters χ_1, χ_2 mod p^m, and f_1, f_2 in $\mathbb{Z}[x]$, the sum $S = \sum_{x=1}^{p^m} \chi_1(x)\chi_2(f_1(x^k))e_{p^m}(f_2(x^k))$ is zero unless $\chi_1 = \chi_3^k$ for some mod p^m character χ_3.*

While it should be noted this condition springs up naturally when evaluating the sums, it is useful to prove it here.

Proof. Taking $z = a^{\phi(p^m)/(k,\phi(p^m))}$, a a primitive root mod p^m, we have $z^k = 1$ and

$$S = \sum_{x=1}^{p^m} \chi_1(xz)\chi_2(f_1((xz)^k))e_{p^m}(f_2((xz)^k)) = \chi_1(z)S.$$

Hence if $S \neq 0$ we must have $1 = \chi_1(z) = \chi_1(a)^{\phi(p^m)/(k,\phi(p^m))}$ and consequently $\chi_1(a)$ is a complex $\phi(p^m)/(k,\phi(p^m))$-th root of unity and so $\chi_1(a) = e_{\phi(p^m)}\left(c'(k,\phi(p^m))\right)$ for some integer c'. Letting c_1 be any integer satisfying

$$c'(k,\phi(p^m)) \equiv c_1 k \bmod \phi(p^m),$$

(c_1 is unique mod $\phi(p^m)/(k,\phi(p^m))$) we equivalently have $\chi_1 = \chi_3^k$ where $\chi_3(a) = e_{\phi(p^m)}(c_1)$. □

2.4 Definitions and Congruence Relationships

2.4.1 The case p is odd

Let a be a primitive root mod p, the existence of which is an elementary result in number theory (see Section 2.8 in [18]). Further from Theorem 2.40 in [18] we know if a is a primitive root mod p^2 it is a primitive root for all higher powers of p as well. For a mod p primitive root, a, we must have a is also a primitive root mod p^2 to get that a is a primitive root mod p^j for all j. By using that $a^{p-1} = 1 + rp$ for some r we take

$$\begin{aligned}(a+\lambda p)^{p-1} &\equiv a^{p-1} + (p-1)p\lambda a^{p-2} \bmod p^2 \\ &\equiv (1+rp) - p\lambda a^{p-2} \bmod p^2 \\ &\equiv 1 + (r - \lambda a^{p-2})p \bmod p^2,\end{aligned}$$

and take λ such that $p \nmid (r - \lambda a^{p-2})$ giving us just the primitive root we are looking for. For this thesis we assume $p \nmid r$ and $\lambda = 0$, thus a is a primitive root for all powers of p. We now define the integers r and R_j by

$$a^{\phi(p)} = 1 + rp, \qquad a^{\phi\left(p^j\right)} = 1 + R_j p^j. \tag{2.8}$$

Note, $p \nmid r$ and for any $j \geq 2$

$$\begin{aligned}a^{\phi(p^j)} = 1 + R_j p^j &= (a^{\phi(p^{j-1})})^p = (1 + R_{j-1}p^{j-1})^p \\ &\equiv 1 + R_{j-1}p^j + \binom{p}{2} R_{j-1}^2 p^{2(j-1)} \bmod p^{3(j-1)}\end{aligned}$$

giving

$$R_j \equiv R_{j-1} \bmod p^{j-1},$$

and thus for any $j \geq i$ we have

$$R_j \equiv R_i \bmod p^i. \tag{2.9}$$

For a character $\chi \bmod p^m$ we implicitly define c by

$$\chi(a) = e_{\phi(p^m)}(c), \tag{2.10}$$

with $1 \leq c \leq \phi(p^m)$. Note, $p \nmid c$ exactly when χ is primitive.

Lemma 2.4.1. *For the p-adic integer*

$$R := p^{-1}\log(1+rp) = p^{-1}\sum_{i=1}^{\infty}\frac{(rp)^i(-1)^{i-1}}{i} \tag{2.11}$$

we have

$$R \equiv R_j \ mod\ p^j.$$

Proof.

$$a^{\phi(p^j)} = (1+rp)^{p^{j-1}} = 1 + R_j p^j,$$

so

$$\log(1+rp)^{p^{j-1}} = \log(1+R_j p^j).$$

By taking the Taylor series expansion of $\log(1+x)$ we get

$$p^{j-1}\log(1+rp) = p^j R = \sum_{i=1}^{\infty}\frac{(R_j p^j)^i(-1)^{i-1}}{i},$$

and thus we have

$$R = \sum_{i=1}^{\infty}\frac{(R_j)^i p^{(i-1)j}(-1)^{i-1}}{i}.$$

If $p^\nu \mid i$ for any i, then plainly $\nu < i - 1$ for all odd p, giving

$$R \equiv R_j \bmod p^j.$$

□

2.4.2 The case $p = 2$ and $m \geq 3$

When p is not odd and $m \geq 3$ we need two generators -1 and $a = 5$ for $\mathbb{Z}_{2^m}^*$ (again see [18], Chapter 2, Section 8), and define R_j, $j \geq 2$, and c by

$$a^{2^{j-2}} = 1 + R_j 2^j, \qquad \chi(a) = e_{2^{m-2}}(c), \tag{2.12}$$

with χ a mod 2^m character, primitive exactly when $2 \nmid c$. Noting that $R_i^2 \equiv 1 \bmod 8$, we get

$$R_{i+1} = R_i + 2^{i-1} R_i^2 \equiv R_i + 2^{i-1} \bmod 2^{i+2}. \tag{2.13}$$

For $j \geq i + 2$ this gives the relationships,

$$R_j \equiv R_{i+2} \equiv R_{i+1} + 2^i \equiv (R_i + 2^{i-1}) + 2^i \equiv R_i - 2^{i-1} \bmod 2^{i+1} \tag{2.14}$$

and

$$R_j \equiv (R_{i-1} + 2^{i-2}) - 2^{i-1} \equiv R_{i-1} - 2^{i-2} \bmod 2^{i+1}. \tag{2.15}$$

2.5 Gauss Sums

We can now define our first and most well known exponential sum, the Gauss sum

$$G(\chi, q) = \sum_{x=1}^{q} \chi(x) e_q(x) \tag{2.16}$$

where χ is a mod q character.

Letting $q = p^m$ where p is prime, explicit evaluations of these sums exist for $m > 1$ (which we will derive in detail in Chapter 3). The cases when the $m = 1$ sum has exact evaluation are few, the most famous example being the quadratic Gauss sum

$$\sum_{x=1}^{p} e_p(x^2) = \begin{cases} \sqrt{p}, & \text{if } p \equiv 1 \bmod 4, \\ i\sqrt{p}, & \text{if } p \equiv 3 \bmod 4, \end{cases}$$

the evaluation of which is involved (for a nice treatment see Chapter 1.3 of [2]). One can equivalently write the quadratic Gauss sum in the form (2.16) using the Legendre symbol,

$$\begin{aligned} \sum_{x=1}^{p} e_p(x^2) &= \sum_{x=1}^{p} \left(1 + \left(\frac{x}{p}\right)\right) e_p(x) = \sum_{x=1}^{p} e_p(x) + \sum_{x=1}^{p} \left(\frac{x}{p}\right) e_p(x) \\ &= \sum_{x=1}^{p} \left(\frac{x}{p}\right) e_p(x) = G(\chi_Q, p), \end{aligned}$$

where recall we use χ_Q to denote the mod p character that coincides with the Legendre symbol. Here we use that $\sum_{x=1}^{p} e_p(x) = 0$, a central notion in the proofs of the main theorems in this dissertation. It is worth stating that, more generally, summing a linear exponential sum modulo q over a complete set of residues is either q or 0. That is

$$\sum_{x=1}^{q} e_q(Ax) = \begin{cases} q, & \text{if } q \mid A, \\ 0, & \text{otherwise.} \end{cases} \tag{2.17}$$

Plainly if q divides A each term in the sum is 1 giving the total sum to be q, if not then

$$\sum_{x=1}^{q} e_q(Ax) = \frac{e_q(A) - e_q(A)^{q+1}}{1 - e_q(A)} = 0.$$

The bulk of this thesis deals with evaluating mixed sums modulo p^α with $\alpha \geq 2$ using

methods of T. Cochrane and Z. Zheng as detailed in [4], where we are able to reduce certain mixed exponential sums and pure character sums to cases similar to (2.17).

2.6 Character Sums and The Duality of Gauss Sums

A pure character sum has the following properties

$$\sum_{x=1}^{p^m} \chi(x) = \begin{cases} \phi(p^m), & \text{if } \chi \text{ is the principal character,} \\ 0, & \text{otherwise.} \end{cases} \tag{2.18}$$

When χ is the principal character it plain the sum is $\phi(p^m)$. To see the sum is zero otherwise we take a to be a primitive root mod p^m when p is odd and write the sum

$$\sum_{x=1}^{p^m} \chi(x) = \sum_{\gamma=1}^{\phi(p^m)} \chi(a^\gamma) = \sum_{\gamma=1}^{\phi(p^m)} e_{\phi(p^m)}(c\gamma),$$

giving an exponential sum over a complete set of residues as in (2.17), giving the result. Similarly for $p = 2$ we write

$$\sum_{x=1}^{p^m} \chi(x) = \sum_{\gamma=1}^{2^{m-2}} \chi(5^\gamma) + \chi(-1) \sum_{\gamma=1}^{2^{m-2}} \chi(5^\gamma) = \sum_{\gamma=1}^{2^{m-2}} e_{2^{m-2}}(c\gamma) + \chi(-1) \sum_{\gamma=1}^{2^{m-2}} e_{2^{m-2}}(c\gamma)$$

the rest follows from (2.17).

Summing over characters gives a similar result. Letting $\chi_1, \ldots, \chi_{\phi(p^m)}$ be all the characters mod p^m we have that

$$\sum_{i=1}^{\phi(p^m)} \chi_i(b) = \begin{cases} 0, & \text{if } b \not\equiv 1 \bmod p^m, \\ \phi(p^m), & \text{if } b \equiv 1 \bmod p^m. \end{cases} \tag{2.19}$$

By the definition of a Dirichlet character if $(b, p) > 1$, $\chi(b) = 0$. Otherwise $b = a^\beta$ for some

$0 \leq \beta \leq \phi(p^m)$ when p is odd, so we can write

$$\sum_{i=1}^{\phi(p^m)} \chi_i(b) = \sum_{i=1}^{\phi(p^m)} \chi_i(a^\beta) = \sum_{i=1}^{\phi(p^m)} e_{\phi(p^m)}(c_i\beta).$$

Since each character sends the primitive root a to a different $1 \leq c_i \leq \phi(p^m)$ we have a sum over a complete set of residues. By (2.17) the sum is zero unless $\phi(p^m) \mid \beta$, in which case $b = a^\beta = (a^{\phi(p^m)})^{\beta'} \equiv 1 \bmod p^m$ for β' such that $\beta = \beta'\phi(p^m)$, and the sum is $\phi(p^m)$.

When $p = 2$, $m \geq 3$, $b = (-1)^w 5^\beta$, with $0 \leq w \leq 1$ and $1 \leq \beta \leq 2^{m-2}$ and we can write,

$$\sum_{i=1}^{2^{m-1}} \chi_i(b) = \sum_{j=1}^{2^{m-2}} \chi_j(5^\beta) + \sum_{j=1}^{2^{m-2}} \chi_j((-1)^w)\chi_j(5^\beta) = \sum_{j=1}^{2^{m-2}} e_{2^{m-2}}(c_j\beta) + \sum_{j=1}^{2^{m-2}} e_2(w)e_{2^{m-2}}(c_j\beta).$$

Since each character sends 5 to a different $1 \leq c_i \leq 2^{m-2}$ we have a sum over a complete set of residues. Again by (2.17) the sum is zero unless $2^{m-2} \mid \beta$, and $w = 0$, giving that $b \equiv 1 \bmod 2^m$.

This brings us to a rather useful lemma for picking out powers mod p^m.

Lemma 2.6.1. *For b such that $(b, p) = 1$, if b is a kth power mod p^m*

$$\sum_{\chi^k = \chi_0} \chi(b) = \begin{cases} D, & \text{if } p \text{ is odd,} \\ (2,k)D, & \text{if } p = 2,\ m \geq 3, \end{cases}$$

where

$$D = \begin{cases} (k, \phi(p^m)), & \text{for } p \text{ odd,} \\ (k, 2^{m-2}), & \text{for } p = 2,\ m \geq 3. \end{cases} \tag{2.20}$$

If b is not a kth power mod p^m

$$\sum_{\chi^k = \chi_0} \chi(b) = 0.$$

Using this Lemma and observing that the number of x's that give the same value as x^k

is D or $(k, 2D)$ if $p = 2$, we can pick off kth powers in the following manner:

$$\sum_{x=1}^{p^m} \chi(g(x^k)) e_{p^m}(f(x^k)) = \sum_{\chi_1^D = \chi_0} \left(\sum_{u=1}^{p^m} \chi_1(u) \right) \chi(g(u)) e_{p^m}(f(u))$$
$$= \sum_{u=1}^{p^m} \sum_{\chi_1^D = \chi_0} \chi_1(u) \chi(g(u)) e_{p^m}(f(u)),$$

which will become very useful for writing our sums in terms of Gauss sums in Chapter 4.

Proof. We have seen there are exactly $\phi(p^m)$ characters mod p^m. We will show that D of these characters are kth powers. For p odd we have a primitive root a mod p^m and we can write any character

$$\chi(a) = e_{\phi(p^m)}(c), \quad 1 \leq c \leq \phi(p^m).$$

Thus if χ is a kth power of some character χ' we have

$$e_{\phi(p^m)}(c'k) = \chi'(a)^k = \chi(a) = e_{\phi(p^m)}(c)$$

for some c'. Thus we are solving for c' in the congruence $c \equiv c'k \bmod \phi(p^m)$ which has $D = (k, \phi(p^m))$ solutions when $D \mid c$. Therefore there are exactly D characters such that

$$\chi^k = \chi^D = \chi_0,$$

(namely the characters with c such that $c = y\phi(p^m)/D$ for $y = 1, \ldots, D$). If b is a kth power mod p^m

$$\sum_{\chi^D = \chi_0} \chi(b) = D.$$

If b is not a kth power mod p^m then $b = a^\beta$ where $D \nmid \beta$, giving

$$\sum_{\chi^D = \chi_0} \chi(b) = \sum_{\chi^D = \chi_0} \chi(a^\beta) = \sum_{y=1}^{D} e_{\phi(p^m)}\left(\frac{y\beta\phi(p^m)}{D}\right) = \sum_{y=1}^{D} e\left(\frac{y\beta}{D}\right) = 0$$

by (2.17).

If $p = 2$, $m \geq 3$ we have that the characters are defined by

$$\chi(-1) = e_2(c_0), \quad 1 \leq c_0 \leq 2, \quad \text{and} \quad \chi(5) = e_{2^{m-2}}(c), \quad 1 \leq c \leq 2^{m-2}.$$

Thus we have kth power characters for the $(k, 2^{m-2}) = D$ solutions to $c \equiv c'k \bmod 2^{m-2}$ when $D \mid c$, along with the $(2, k)$ solutions to $c_0 \equiv c_0' k \bmod 2$ when $(2, k) \mid c_0$. If $(k, 2) = 1$ then $D = 1$ and there is only the principal character with $\chi^D = \chi_0$, if $(k, 2) = 2$ there are $2D$ characters with this property. Thus if b is a kth power mod 2^m

$$\sum_{\chi^D = \chi_0} \chi(b) = \begin{cases} 2D, & \text{if } (k,2) > 1, \\ 1, & \text{if } (k,2) = 1. \end{cases}$$

If b is not a kth power then $b = (-1)^w 5^\beta$ where $(k, 2) \nmid w$ and $D \nmid \beta$, giving

$$\begin{aligned} \sum_{\chi^D = \chi_0} \chi(b) = \sum_{\chi^D = \chi_0} \chi(-1)^w \chi(5)^\beta &= \sum_{x=1}^{(k,2)} e_2(xw) \sum_{y=1}^{D} e_{2^{m-2}}\left(\frac{y\beta 2^{m-2}}{D}\right) \\ &= \sum_{x=1}^{(k,2)} e_2(xw) \sum_{y=1}^{D} e\left(\frac{y\beta}{D}\right) = 0. \end{aligned}$$

by (2.17). □

The Duality of the Gauss Sum is another useful property given in the following lemma.

Lemma 2.6.2. *If χ is a primitive character mod p^j, $j \geq 1$, then*

$$\sum_{y=1}^{p^j} \chi(y) e_{p^j}(Ay) = \overline{\chi}(A) G(\chi, p^j).$$

Proof. For $p \nmid A$ this is plain from $y \mapsto A^{-1}y$. If $p \mid A$ and $j = 1$ the sum equals $\sum_{y=1}^{p} \chi(y) = 0$. For $j \geq 2$ as χ is primitive there exists a $z \equiv 1 \bmod p^{j-1}$ with $\chi(z) \neq 1$, (there must be

some $a \equiv b \bmod p^{j-1}$ with $\chi(a) \neq \chi(b)$, and we can take $z = ab^{-1}$) so, since $Az \equiv A \bmod p^j$,

$$\sum_{y=1}^{p^j} \chi(y) e_{p^j}(Ay) = \sum_{y=1}^{p^j} \chi(zy) e_{p^j}(Azy) = \chi(z) \sum_{y=1}^{p^j} \chi(y) e_{p^j}(Ay) \tag{2.21}$$

and $\sum_{y=1}^{p^j} \chi(y) e_{p^j}(Ay) = 0$.

An alternate way of showing this for $j \geq 2$ and p odd is writing $y = a^{u+\phi(p^{j-1})v}$, for a a primitive root mod p^m, $\chi(a) = e_{\phi(p^j)}(c)$, $u = 1, ..., \phi(p^{j-1})$, $v = 1, .., p$,

$$\sum_{y=1}^{p^j} \chi(y) e_{p^j}(Ay) = \sum_{u=1}^{\phi(p^{j-1})} \chi(a^u) e_{p^j}(Aa^u) \sum_{v=1}^{p} e_p(cv) = 0. \tag{2.22}$$

□

2.7 Reduction Method of Cochrane and Zheng

In [4] Cochrane and Zheng establish a reduction method for evaluating exponential sums of the form

$$S(\chi, x, f(x), p^m) = \sum_{x=1}^{p^m} \chi(x) e_{p^m}(f(x)) \tag{2.23}$$

which was then generalized to sums of the form

$$S(\chi, g(x), f(x), p^m) = \sum_{x=1}^{p^m} \chi(g(x)) e_{p^m}(f(x))$$

in [5] with g, f rational functions over $\mathbb{Z}$. The method for evaluating (2.23) involves finding the set, $\mathcal{A}$, of all nonzero residues mod p satisfying the congruence

$$p^{-t_1}(rxf'(x) + c) \equiv 0 \bmod p \tag{2.24}$$

(with the integers r and c defined in (2.8) and (2.10)), where $p^{t_1} \mid\mid rXf'(X)+c$. We write

$$S(\chi, x, f, p^m) = \sum_{x=1}^{p^m} \chi(x) e_{p^m}(f(x)) = \sum_{\alpha=1}^{p-1} S_\alpha,$$

where for any integer α with $p \nmid \alpha$,

$$S_\alpha = S_\alpha(\chi, x, f, p^m) := \sum_{\substack{x=1 \\ x \equiv \alpha \bmod p}}^{p^m} \chi(x) e_{p^m}(f(x)).$$

Theorem 2.7.1 (T. Cochrane, Z. Zheng [4]). *Let p be an odd prime, f be any polynomial over $\mathbb{Z}$ and t_1 be as above and t such that $p^t \mid\mid f'$. Suppose that $m \geq t_1 + 2$. Then for any integer α with $p \nmid \alpha$ we have*

1. *If $\alpha \notin \mathcal{A}$, $S_\alpha(\chi, f, p^m) = 0$.*

2. *If α is a critical point of multiplicity $\nu \geq 1$ then $t = t_1$ and*

$$|S_\alpha(\chi, x, f, p^m)| \leq \nu p^{\frac{t}{\nu+1}} p^{m(1-\frac{1}{\nu+1})}. \tag{2.25}$$

3. *If α is a critical point of multiplicity one then*

$$S_\alpha(\chi, x, f, p^m) = \begin{cases} \chi(\alpha^*) e_{p^m}(f(\alpha^*))\, p^{\frac{m+t}{2}}, & \text{If } m-t \text{ is even,} \\ \chi(\alpha^*) e_{p^m}(f(\alpha^*))\, \chi_2(A_\alpha) G(\chi_Q, p)\, p^{\frac{m+t-1}{2}}, & \text{if } m-t \text{ is odd,} \end{cases}$$

where α^* is the unique lifting of α to a solution of the congruence $p^{-t}(Rcf'(x)+c) \equiv 0 \bmod p^{[(m-t+1)/2]}$, and $A_\alpha \equiv 2\alpha p^{-t}(f'(\alpha) + \alpha f''(\alpha)) \bmod p$. In particular, we have equality in (2.25).

Here χ_Q is the Legendre symbol (2.4) and so $G(\chi_Q, p)$ is the quadratic Gauss sum discussed earlier, and R is the p-adic integer $R := p^{-1}\log(1+rp)$.

When $f(x) = nx^k$ with $p \nmid k$ we have the twisted gauss sum

$$\sum_{x=1}^{p^m} \chi(x) e_{p^m}\left(nx^k\right) \tag{2.26}$$

and (2.24) takes the simple form

$$rkx^k + c \equiv 0 \mod p, \tag{2.27}$$

we have that either (2.26) is zero or a sum of $(p-1,k)$ S_α sums, depending whether there is a solution to (2.27) or not. When the critical points have multiplicity one the S_α can be evaluated explicitly. For example if $f(x) = x$ then as observed in Cochrane and Zheng [4, §9] the critical point congruence is simply $rx + c \equiv 0 \mod p$. For p odd and $m \geq 2$, if χ is imprimitive there is no critical point and $S(\chi, x, p^m) = 0$, while if χ is primitive there is one critical point of multiplicity one and

$$S(\chi, x, p^m) = \chi(\alpha^*) e_{p^m}(\alpha^*) p^{m/2} \left(\frac{-2rc}{p^m}\right) \epsilon, \tag{2.28}$$

where $\left(\frac{x}{p^m}\right)$ denotes the Jacobi symbol,

$$\varepsilon_{p^m} := \begin{cases} 1, & \text{if } p^m \equiv 1 \mod 4, \\ i, & \text{if } p^m \equiv 3 \mod 4, \end{cases} \tag{2.29}$$

and

$$R\alpha^* \equiv -c \mod p^{[(m+1)/2]}. \tag{2.30}$$

(A small adjustment is needed in (2.30) in the case $p = m = 3$, see (5.15), and more generally in [4, Theorem 1.1(iii)] when $p = m - t = 3$). The same formula (2.28) occurs in Mauclaire [16] with α^* defined by $\chi(1 + p^{m/2}) = e_{p^{m/2}}(-\alpha^*)$ when m is even and $\chi(1 +$

$p^{(m-1)/2} + 2^{-1}p^{m-1}) = e_{p^{(m+1)/2}}(-\alpha^*)$ when m is odd. Mauclaire also deals with the case $p = 2$ in the second part of [16]. A variation of (2.28) was obtained by Odoni [19] (see also Berndt, Evans and Williams [2, Theorems 1.6.2-1.6.4]). In Chapter 3 we will evaluate the $f(x) = x$ sum using the reduction method but replacing p-adic integer R with a slightly simpler constant, as well as dealing with the case $p = 2$. In the later chapters we will be evaluating sums with critical points of multiplicity greater than one and obtaining explicit evaluations.

Chapter 3

Evaluation of Gauss Sums

The mod p^m Gauss sum is given as

$$G(\chi, p^m) = \sum_{x=1}^{p^m} \chi(x) e_{p^m}(x)$$

In this chapter we will give an explicit evaluation of the Gauss sum for all p, illustrating the reduction methods of Cochrane and Zheng discussed in 2.7. By using the congruence relationships in 2.4 we get an evaluation particularly useful for the explicit evaluation of the general Jacobi sum,

$$J_{p^n}(\chi_1, \ldots, \chi_k, p^m) = \sum_{x_1=1}^{p^m} \cdots \sum_{\substack{x_k=1 \\ x_1+\cdots+x_k=p^n}}^{p^m} \chi_1(x_1) \cdots \chi_k(x_k), \quad m > n,$$

in Chapter 7.

3.1 Evaluation of the Gauss Sum

We shall need an explicit evaluation of the mod p^m, $m \geq 2$, Gauss sums. The form we use comes from applying the technique of Cochrane & Zheng [4] as formulated in [20]. For odd

p this is essentially the same as [5, §9] but for $p = 2$ seems new. Variations can be found in Odoni [19] and Mauclaire [16] (see also [2, Chapter 1]).

Theorem 3.1.1. *Suppose that χ is a mod p^m character with $m \geq 2$. If χ is imprimitive, then $G(\chi, p^m) = 0$. If χ is primitive, then*

$$G(\chi, p^m) = p^{\frac{m}{2}} \chi\left(-cR_j^{-1}\right) e_{p^m}\left(-cR_j^{-1}\right) \begin{cases} \left(\frac{-2rc}{p}\right)^m \varepsilon_{p^m}, & \text{if } p \neq 2, \text{ and } p^m \neq 3^3, \\ \left(\frac{2}{c}\right)^m \omega^c, & \text{if } p = 2 \text{ and } m \geq 5, \end{cases} \tag{3.1}$$

for any $j \geq \lceil \frac{m}{2} \rceil$ when p is odd and any $j \geq \lceil \frac{m}{2} \rceil + 2$ when $p = 2$.

For the remaining cases

$$G(\chi, 27) = 3^{\frac{3}{2}} \chi\left(-cR_j^{-1}\right) e_{3^3}\left(-10cR_j^{-1}\right) \left(\frac{-2rc}{3}\right) i,$$

and

$$G(\chi, 2^m) = 2^{\frac{m}{2}} \begin{cases} i, & \text{if } m = 2, \\ \omega^{1-\chi(-1)}, & \text{if } m = 3, \\ \chi(-c) e_{16}(-c), & \text{if } m = 4. \end{cases} \tag{3.2}$$

Here x^{-1} denotes the inverse of x mod p^m, and r, R_j and c are as in (2.8) and (2.10) or (2.12) and $\omega := e^{\pi i/4}$.

It is important to note that although we are evaluating the Gauss sum using an arbitrary R_j during the course of the proof we get the evaluation

$$G(\chi, p^m) = p^{\frac{m}{2}} \chi(\alpha) e_{p^m}(\alpha) \begin{cases} \left(\frac{-2rc}{p}\right)^m \varepsilon_{p^m}, & \text{if } p \neq 2,\ p^m \neq 3^3, \\ 1, & \text{if } p = 2 \text{ and } m \geq 5 \text{ is even}, \\ \left(\frac{1-i^c}{\sqrt{(2)}}\right), & \text{if } p = 2 \text{ and } m \geq 5 \text{ is odd}, \end{cases} \tag{3.3}$$

where α is a solution to

$$c + R_{\lceil \frac{m}{2} \rceil} x \equiv 0 \bmod p^{\lceil \frac{m}{2} \rceil}, \tag{3.4}$$

unless χ is imprimitive in which case there is no solution to (3.4), relatively prime to p and $G(\chi, p^m) = 0$. The Gauss sum evaluation of the theorem becomes useful when evaluating (1.4) in Chapter 7.

Proof. For p odd, let a be a primitive root of p for all powers of p. We can write

$$G(\chi, p^m) = \sum_{x=1}^{p^m} \chi(x) e_{p^m}(x) = \sum_{\gamma=1}^{\phi(p^m)} \chi(a^\gamma) e_{p^m}(a^\gamma).$$

For an interval I_1 of length $\phi(p^{\lceil \frac{m}{2} \rceil})$ it is clear that

$$\gamma = \phi(p^{\lceil \frac{m}{2} \rceil}) u + v$$

with $u \in I_2 = \left[1, p^{\lfloor \frac{m}{2} \rfloor}\right]$, $v \in I_1$, runs through a complete set of residues mod $\phi(p^m)$. Hence,

$$\begin{aligned} G(\chi, p^m) &= \sum_{v \in I_1} \chi(a^v) \sum_{u \in I_2} \chi(a^{\phi(p^{\lceil \frac{m}{2} \rceil}) u}) e_{p^m}\left(a^{\phi(p^{\lceil \frac{m}{2} \rceil}) u + v}\right) \\ &= \sum_{v \in I_1} \chi(a^v) \sum_{u \in I_2} e_{p^{\lfloor \frac{m}{2} \rfloor}}(cu) e_{p^m}\left((1 + R_{\lceil \frac{m}{2} \rceil} p^{\lceil \frac{m}{2} \rceil})^u a^v\right). \end{aligned}$$

Observing $(1 + R_{\lceil \frac{m}{2} \rceil} p^{\lceil \frac{m}{2} \rceil})^u \equiv 1 + R_{\lceil \frac{m}{2} \rceil} p^{\lceil \frac{m}{2} \rceil} u \bmod p^m$ gives

$$\begin{aligned} G(\chi, p^m) &= \sum_{v \in I_1} \chi(a^v) \sum_{u \in I_2} e_{p^{\lfloor \frac{m}{2} \rfloor}}(cu) e_{p^m}\left((1 + R_{\lceil \frac{m}{2} \rceil} p^{\lceil \frac{m}{2} \rceil} u) a^v\right) \\ &= \sum_{v \in I_1} \chi(a^v) e_{p^m}(a^v) \sum_{u \in I_2} e_{p^{\lfloor \frac{m}{2} \rfloor}}(cu) e_{p^m}\left(R_{\lceil \frac{m}{2} \rceil} p^{\lceil \frac{m}{2} \rceil} u a^v\right) \\ &= \sum_{v \in I_1} \chi(a^v) e_{p^m}(a^v) \sum_{u \in I_2} e_{p^{\lfloor \frac{m}{2} \rfloor}}\left(u(c + R_{\lceil \frac{m}{2} \rceil} a^v)\right). \end{aligned}$$

Noting that the u sum is over a complete set of residues mod $p^{\lfloor \frac{m}{2} \rfloor}$ gives $G(\chi, p^m) = 0$ unless

$$c + R_{\lceil \frac{m}{2} \rceil} a^v \equiv 0 \bmod p^{\lfloor \frac{m}{2} \rfloor}, \tag{3.5}$$

has a solution $\alpha = a^{v_0}$. If $p \mid c$ there is no solution and $G(\chi, p^m) = 0$. When $p \nmid c$, there exists a solutions when $\alpha \equiv -cR^{-1}_{\lceil \frac{m}{2} \rceil} \bmod p^{\lfloor \frac{m}{2} \rfloor}$. To simplify our result we choose α to be a solution to the stronger congruence

$$c + R_J x \equiv 0 \bmod p^J, \tag{3.6}$$

where $J := \left\lceil \frac{m}{2} \right\rceil$, to satisfy (3.5). Given any two solutions, a^{v_0} and a^{v_1}, to (3.5) we have

$$a^{v_0} \equiv a^{v_1} \bmod p^{\lfloor \frac{m}{2} \rfloor}$$

or equivalently

$$v_0 \equiv v_1 \bmod \phi(p^{\lfloor \frac{m}{2} \rfloor}).$$

When m is even $\lfloor \frac{m}{2} \rfloor = \lceil \frac{m}{2} \rceil$ thus there can only be one solution in the range of v. Taking I_1 to contain a^{v_0} gives the result for m even. When m is odd, given a solution a^{v_0}, we have $a^{v_0 + y\phi(p^{\lfloor \frac{m}{2} \rfloor})}$ for $y = 1, \ldots, p$ are all the solutions in an interval of length $\phi(p^{\lceil \frac{m}{2} \rceil})$. Taking I_1 to contain these solutions and letting $L = \lfloor \frac{m}{2} \rfloor = \frac{m-1}{2}$ we get

$$\begin{aligned} G(\chi, p^m) &= p^L \sum_{y=1}^{p} \chi(a^{v_0 + y\phi(p^L)}) e_{p^m}\left(a^{v_0 + y\phi(p^L)}\right) \\ &= p^L \chi(a^{v_0}) \sum_{y=1}^{p} \chi(a^{y\phi(p^L)}) e_{p^m}\left(a^{v_0}(1 + R_L p^L)^y\right) \\ &= p^L \chi(a^{v_0}) \sum_{y=1}^{p} e_{p^{\lceil \frac{m}{2} \rceil}}(cy)\, e_{p^m}\left(a^{v_0}(1 + R_L p^L)^y\right). \end{aligned}$$

As long as $m \geq 3$ we have

$$\begin{aligned}(1+R_Lp^L)^y &= 1 + yR_Lp^L + \binom{y}{2}R_L^2p^{m-1} + \binom{y}{3}R_L^3p^{3\frac{(m-1)}{2}} + \dots \\ &\equiv 1 + (R_Lp^L - 2^{-1}R_L^2p^{m-1})y + 2^{-1}R_L^2p^{m-1}y^2 \mod p^m\end{aligned}$$

Thus

$$\begin{aligned}G(\chi, p^m) &= p^L\chi(a^{v_0})e_{p^m}\left(a^{v_0}\right)\sum_{y=1}^{p} e_{p^{\lceil \frac{m}{2} \rceil}}\left(cy\right)e_{p^m}\left(a^{v_0}((R_Lp^L - 2^{-1}R_L^2p^{m-1})y + 2^{-1}R_L^2p^{m-1}y^2)\right) \\ &= p^L\chi(a^{v_0})e_{p^m}\left(a^{v_0}\right)\sum_{y=1}^{p} e_{p^{\lceil \frac{m}{2} \rceil}}\left(y(c+R_La^{v_0})\right)e_{p^m}\left(a^{v_0}(-2^{-1}R_L^2p^{m-1}y + 2^{-1}R_L^2p^{m-1}y^2)\right).\end{aligned} \tag{3.7}$$

We here note that $R_L \equiv R_J + 2^{-1}R_L^2p^L - 3^{-1}R_L^3p^{m-1} \mod p^J$ where the last term is zero unless $p = 3$, $m = 3$. This can be seen from

$$\begin{aligned}1 + R_Jp^J = a^{\phi(p^J)} = a^{\phi(p^L)p} &= (1+R_Lp^L)^p \\ &\equiv 1 + pR_Lp^L + \binom{p}{2}R_L^2p^{2L} + \binom{p}{3}R_L^3p^{3L} \\ &\equiv 1 + p^J\left(R_L - 2^{-1}R_L^2p^L + 3^{-1}R_L^3p^{m-1}\right) \mod p^{m+1},\end{aligned}$$

implying that

$$R_J \equiv R_L - 2^{-1}R_L^2p^L + 3^{-1}R_L^3p^{m-1} \mod p^{(m+1)-J}.$$

Using this congruence as well as the fact that a^{v_0} is a solution to the stronger characteristic

equation (3.6) we have

$$\begin{aligned} e_{p^{\lceil \frac{m}{2} \rceil}}\left(y(c+R_L a^{v_0})\right) &= e_{p^{\lceil \frac{m}{2} \rceil}}\left(y(c+a^{v_0}(R_J+2^{-1}R_L^2 p^L - 3^{-1}R_L^3 p^{m-1}))\right) \\ &= e_{p^{\lceil \frac{m}{2} \rceil}}\left(ya^{v_0}(2^{-1}R_L^2 p^L - 3^{-1}R_L^3 p^{m-1})\right) \\ &= e_{p^m}\left(ya^{v_0}(2^{-1}R_L^2 p^{m-1} - 3^{-1}R_L^3 p^{3\frac{m-1}{2}})\right). \end{aligned}$$

Thus the y sum becomes, (when not in the special case $p=3, m=3$)

$$\begin{aligned} &\sum_{y=1}^{p} e_{p^m}\left(ya^{v_0}(2^{-1}R_L^2 p^{m-1})\right) e_{p^m}\left(a^{v_0}(-2^{-1}R_L^2 p^{m-1}y + 2^{-1}R_L^2 p^{m-1}y^2)\right) \\ &\quad = \sum_{y=1}^{p} e_p\left(a^{v_0}2^{-1}R_L^2(y^2)\right) \\ &\quad = \left(\frac{a^{v_0}2^{-1}R_L^2}{p}\right)\sum_{y=1}^{p} e_p\left(y^2\right) \\ &\quad = \left(\frac{-2cr}{p}\right)\sum_{y=1}^{p} e_p\left(y^2\right) = \left(\frac{-2cr}{p}\right) G\left(\chi_Q, p\right). \end{aligned}$$

Here $G\left(\chi_Q, p\right).$ is the quadratic gauss sum which famously sums to $\sqrt{p}$ or $i\sqrt{p}$ as $p \equiv 1$ or 3 mod 4. Note that for a solution, a^{v_0}, to the equation

$$c + R_J x \equiv 0 \bmod p^J,$$

by (2.9) we may take $a^{v_0} = -cR_J^{-1} \equiv -cR_j^{-1} \bmod p^J$ for any $j \geq J$ and $-cR_j^{-1}$ will be a solution as well. This together with (3.7) gives the result for p odd except when $p = m = 3$.

When $p=3$, $m=3$ we get the y sum

$$\begin{aligned}
&\sum_{y=1}^{3} e_{27}\left(ya^{v_0}(2^{-1}R_L^2 9 - R_L^3 9)\right) e_{27}\left(a^{v_0}(-2^{-1}R_L^2 9y + 2^{-1}R_L^2 9y^2)\right) \\
&\qquad = \sum_{y=1}^{3} e_3\left(a^{v_0}2^{-1}R_L^2(y^2) - R_L^3 a^{v_0} y\right) \\
&\qquad = \sum_{y=1}^{3} e_3\left(a^{v_0}2^{-1}(y^2 + R_L y)\right) = e_3\left(-a^{v_0}2^{-1}\right)\sum_{y=1}^{3} e_3\left(a^{v_0}2^{-1}(y + 2^{-1}R_l)^2\right) \\
&\qquad = e_3\left(a^{v_0}\right)\sum_{w=1}^{3} e_3\left(-a^{v_0}w^2\right) = 3^{1/2}\left(\frac{-2rc}{3}\right) e_3\left(-cR_{\lceil \frac{m}{2}\rceil}^{-1}\right) i
\end{aligned}$$

completing the p odd case.

For $p=2$, $m \geq 6$ similarly write the sum in terms of the generators -1 and 5 giving,

$$G(\chi, 2^m) = \sum_{x=1}^{2^m} \chi(x) e_{2^m}(x) = \sum_{A\in\{-1,1\}} \sum_{\gamma=1}^{2^{m-2}} \chi(A5^\gamma) e_{2^m}(A5^\gamma).$$

We let $\gamma = u2^{\lceil \frac{m}{2}\rceil - 2} + v$ where $v \in I_1$ and $u \in I_2$ where I_1 is an interval of length $2^{\lceil \frac{m}{2}\rceil - 2}$ and $I_2 = \left[1, 2^{\lfloor \frac{m}{2}\rfloor}\right]$. Thus after simplification similar to the p odd case we have

$$\begin{aligned}
G(\chi, 2^m) &= \sum_{A\in\{-1,1\}} \sum_{v\in I_1} \chi(A5^v) \sum_{u\in I_2} e_{2^{\lfloor \frac{m}{2}\rfloor}}(cu)\, e_{2^m}\left(A5^v\left(1 + R_{\lceil \frac{m}{2}\rceil} 2^{\lceil \frac{m}{2}\rceil}\right)^u\right) \\
&= \sum_{A\in\{-1,1\}} \sum_{v\in I_1} \chi(A5^v) \sum_{u\in I_2} e_{2^{\lfloor \frac{m}{2}\rfloor}}(cu)\, e_{2^m}\left(A5^v + A5^v u R_{\lceil \frac{m}{2}\rceil} 2^{\lceil \frac{m}{2}\rceil}\right) \\
&= \sum_{A\in\{-1,1\}} \sum_{v\in I_1} \chi(A5^v) e_{2^m}(A5^v) \sum_{u\in I_2} e_{2^{\lfloor \frac{m}{2}\rfloor}}(cu)\, e_{2^m}\left(A5^v u R_{\lceil \frac{m}{2}\rceil} 2^{\lceil \frac{m}{2}\rceil}\right) \\
&= \sum_{A\in\{-1,1\}} \sum_{v\in I_1} \chi(A5^v) e_{2^m}(A5^v) \sum_{u\in I_2} e_{2^{\lfloor \frac{m}{2}\rfloor}}\left(u\left(c + A5^v R_{\lceil \frac{m}{2}\rceil}\right)\right).
\end{aligned}$$

So $G(\chi, 2^m) = 0$ unless we have a solution to either the $A = 1$ or -1 characteristic equation

$$c + A5^v R_{\lceil \frac{m}{2}\rceil} \equiv 0 \bmod 2^{\lfloor \frac{m}{2}\rfloor}. \tag{3.8}$$

Notice that both $c \pm 5^v R_{\lceil \frac{m}{2} \rceil} \equiv 0 \bmod 2^{\lfloor \frac{m}{2} \rfloor}$ cannot be simultaneously satisfied as $-5^{v_1} \not\equiv 5^{v_2} \bmod 2^{\lfloor \frac{m}{2} \rfloor}$ so $-cR^{-1}_{\lceil \frac{m}{2} \rceil}$ is either 5^v or -5^v for some v. Clearly we can have no solution to equation (3.8) if $2 \mid c$, thus χ must be a primitive character. For the sake of simplification we take our solutions to be solutions of the stronger characteristic equation

$$c + A5^v R_{\lceil \frac{m}{2} \rceil} \equiv 0 \bmod 2^{\lceil \frac{m}{2} \rceil}. \tag{3.9}$$

For two solutions $A_0 5^{v_0}$ and $A_0 5^{v_1}$, we have

$$5^{v_0} \equiv 5^{v_1} \bmod 2^{\lfloor \frac{m}{2} \rfloor}.$$

Thus

$$v_0 \equiv v_1 \bmod 2^{\lfloor \frac{m}{2} \rfloor - 2},$$

which is precisely the length of I_1 when m is even. Taking I_1 to contain this solution we get

$$G(\chi, 2^m) = 2^{m/2} \chi\left(A_0 5^{v_0}\right) e_{2^m}\left(A_0 5^{v_0}\right). \tag{3.10}$$

For m odd we take I_2 to contain the two solutions, $A_0 5^{v_0}$ and $A_0 5^{v_0 + 2^{\lfloor \frac{m}{2} \rfloor - 2}}$ giving

$$\begin{aligned}
G(\chi, 2^m) &= 2^{\lfloor \frac{m}{2} \rfloor} \left(\chi(A5^{v_0}) e_{2^m}\left(A_0 5^{v_0}\right) + \chi\left(A_0 5^{v_0 + 2^{\lfloor \frac{m}{2} \rfloor - 2}}\right) e_{2^m}\left(A_0 5^{v_0 + 2^{\lfloor \frac{m}{2} \rfloor - 2}}\right) \right) \\
&= 2^{\lfloor \frac{m}{2} \rfloor} \left(\chi(A_0 5^{v_0}) e_{2^m}\left(A_0 5^{v_0}\right) + \chi\left(A_0 5^{v_0 + 2^{\lfloor \frac{m}{2} \rfloor - 2}}\right) e_{2^m}\left(A_0 5^{v_0 + 2^{\lfloor \frac{m}{2} \rfloor - 2}}\right) \right) \\
&= 2^{\lfloor \frac{m}{2} \rfloor} \chi(A_0 5^{v_0}) e_{2^m}\left(A_0 5^{v_0}\right) \left(1 + \chi\left(5^{2^{\lfloor \frac{m}{2} \rfloor - 2}}\right) e_{2^m}\left(A_0 5^{v_0 + 2^{\lfloor \frac{m}{2} \rfloor - 2}} - A_0 5^{v_0}\right) \right) \\
&= 2^{\lfloor \frac{m}{2} \rfloor} \chi(A_0 5^{v_0}) e_{2^m}\left(A_0 5^{v_0}\right) \left(1 + \chi\left(5^{2^{\lfloor \frac{m}{2} \rfloor - 2}}\right) e_{2^m}\left(A_0 5^{v_0} R_{\lfloor \frac{m}{2} \rfloor} 2^{\lfloor \frac{m}{2} \rfloor}\right) \right) \\
&= 2^{\lfloor \frac{m}{2} \rfloor} \chi(A_0 5^{v_0}) e_{2^{\lceil \frac{m}{2} \rceil}}\left(A_0 5^{v_0}\right) \left(1 + e_{2^{\lceil \frac{m}{2} \rceil}}\left(c + A_0 5^{v_0} R_{\lfloor \frac{m}{2} \rfloor}\right) \right).
\end{aligned}$$

We know from (2.13) that $R_{\lfloor \frac{m}{2} \rfloor} \equiv R_{\lceil \frac{m}{2} \rceil} - 2^{\lfloor \frac{m}{2} \rfloor - 1} R^2_{\lfloor \frac{m}{2} \rfloor} \bmod 2^{\lceil \frac{m}{2} \rceil + 1}$. Coupled with the

solution to the stronger characteristic equation from (3.9) we get

$$\begin{aligned} c + A_0 5^{v_0} R_{\lfloor \frac{m}{2} \rfloor} &= c + A_0 5^{v_0} \left(R_{\lceil \frac{m}{2} \rceil} - 2^{\lfloor \frac{m}{2} \rfloor - 1} R^2_{\lfloor \frac{m}{2} \rfloor} \right) \\ &\equiv -A_0 5^{v_0} 2^{\lfloor \frac{m}{2} \rfloor - 1} \bmod 2^{\lceil \frac{m}{2} \rceil} \end{aligned}$$

since $R_j^2 \equiv 1 \bmod 4$ for $j \geq 2$. Using this gives

$$e_{2^{\lceil \frac{m}{2} \rceil}} \left(c + A_0 5^{v_0} R_{\lfloor \frac{m}{2} \rfloor} \right) = e_{2^2} \left(-A_0 5^{v_0} \right) = e_{2^2} \left(c R^{-1}_{\lceil \frac{m}{2} \rceil} \right) = -i^c,$$

as $R_j \equiv -1 \bmod 4$ for any $j \geq 3$. Thus for $p = 2$ we have

$$G(\chi, p^m) = 2^{m/2} \chi(\alpha) e_{2^m}(\alpha) \begin{cases} 1, & \text{if } m \text{ is even,} \\ \left(\frac{1 - i^c}{\sqrt{2}} \right), & \text{if } m \text{ is odd,} \end{cases} \tag{3.11}$$

where α is a solution to

$$c + R_J x \equiv 0 \bmod 2^J, \tag{3.12}$$

and zero if there is no solution or χ is imprimitive. If $2 \nmid c$ and $j \geq J + 2$ then (using (2.14) and $R_j \equiv -1 \bmod 4$, $j \geq 3$) we can take

$$\alpha \equiv -c R_J^{-1} \equiv -c (R_j + 2^{J-1})^{-1} \equiv -c (R_j^{-1} - 2^{J-1}) \bmod 2^{J+1},$$

and

$$\chi(\alpha) e_{2^m}(\alpha) = \chi(-c R_j^{-1}) e_{2^m}(-c R_j^{-1}) \chi(1 - R_j 2^{J-1}) e_{2^m}(c 2^{J-1}),$$

where, checking the four possible $c \bmod 8$,

$$\left(\frac{1 - i^c}{\sqrt{2}} \right) = \omega^{-c} \left(\frac{2}{c} \right).$$

Now

$$e_{2^m}(c2^{J-1}) = e_{2^{m-2}}(c2^{J-3}) = \chi\left(5^{2^{J-3}}\right) = \chi\left(1 + R_{J-1}2^{J-1}\right),$$

where, since $R_j \equiv R_{J-1} - 2^{J-2} \bmod 2^{J+1}$,

$$\begin{aligned}\left(1 - R_j 2^{J-1}\right)\left(1 + R_{J-1}2^{J-1}\right) &= 1 + (R_{J-1} - R_j)2^{J-1} - R_j R_{J-1} 2^{2J-2} \\ &\equiv 1 + 2^{2J-3} + R_{J-1}2^{2J-2} \equiv 1 + R_{2J-3}2^{2J-3} \bmod 2^m.\end{aligned}$$

Hence

$$\chi(1 - R_j 2^{J-1}) e_{2^m}(c2^{J-1}) = \chi\left(5^{2^{2J-5}}\right) = e_{2^{m-2}}(c2^{2J-5}) = \begin{cases} \omega^c, & \text{if } m \text{ is even,} \\ \omega^{2c}, & \text{if } m \text{ is odd.} \end{cases}$$

One can check numerically that the formula still holds for the 2^{m-2} primitive mod 2^m characters when $m = 5$. For $m = 2, 3, 4$ one has (3.2) instead of $2i\omega$, $2^{\frac{3}{2}}\omega^2$, $2^2\chi(c)e_{2^4}(c)\omega^c$ (so our formula (3.1) requires an extra factor ω^{-1}, $\omega^{-1-\chi(-1)}$ or $\chi(-1)\omega^{-2c}$ respectively).

□

Chapter 4

Rewriting Sums in Terms of Gauss Sums to Obtain Weil and Weil Type Bounds

For a general mixed exponential sum of the form

$$S(\chi, g(x), f(x), p) = \sum_{x=1}^{p} \chi(g(x)) e_p(f(x))$$

with f, g rational with the poles of g omitted, a rather well known result of Weil [24] is the upper bound on such sums. If f is a polynomial and the sum is non-degenerate then

$$|S(\chi, g(x), f(x), p)| \leq (\deg(f) + \ell - 1)\, p^{1/2}, \tag{4.1}$$

where ℓ denotes the number of zeros and poles of g (see Castro & Moreno [3] or Cochrane & Pinner [8] for a treatment of the general case). Here we are dealing with special sums that can be written in terms of Gauss sums which can be used to give the Weil bound in the mod p case and Weil type bounds for general prime powers, which in certain cases are

sharp.

4.1 Gauss Sums and Weil type bounds

For a character χ mod p^j, $j \geq 1$, we let $G(\chi, p^j)$ denote the Gauss sum

$$G(\chi, p^j) = \sum_{x=1}^{p^j} \chi(x) e_{p^j}(x).$$

Recall (see for example Section 1.6 of Berndt, Evans & Williams [2]) that

$$\left|G(\chi, p^j)\right| = \begin{cases} p^{j/2}, & \text{if } \chi \text{ is primitive mod } p^j, \\ 1, & \text{if } \chi = \chi_0 \text{ and } j = 1, \\ 0, & \text{otherwise.} \end{cases} \tag{4.2}$$

For the classical mod p Gauss sum, letting $d = (k, p-1)$ we can write

$$\begin{aligned} \sum_{x=0}^{p-1} e_p(Ax^k) &= 1 + \sum_{x=1}^{p-1} e_p(Ax^d) \\ &= 1 + \sum_{\chi^d = \chi_0} \sum_{u=1}^{p-1} \chi(u) e_p(Au) \\ &= 1 + \sum_{\substack{\chi^d = \chi_0 \\ \chi \neq \chi_0}} \overline{\chi}(A) G(\chi, p) - 1 \\ &= \sum_{\substack{\chi^d = \chi_0 \\ \chi \neq \chi_0}} \overline{\chi}(A) G(\chi, p) \end{aligned}$$

by Lemma 2.6.2, and Lemma 2.6.1. From (4.2) we get exactly the Weil bound of

$$\left| \sum_{x=0}^{p-1} e_p(Ax^k) \right| \leq (d-1) p^{\frac{1}{2}}.$$

In this chapter we show the sums we are considering can all be written in terms of prime power Gauss sums.

4.2 Twisted monomial sums as Gauss Sums

In this section we write the twisted monomial Gauss

$$S_1 = S_1(\chi, x, nx^k, p^m) = \sum_{x=1}^{p^m} \chi(x) e_{p^m}\left(nx^k\right)$$

in terms of Gauss sums. Here the Weil bound comes from writing S_1 as a sum of $(k, \phi(p^m))$ (when p is odd) and $(2,k)(k, 2^{m-2})$ (when $p = 2$) sums of absolute value $\sqrt{p}$, giving

$$\left|S_1(\chi, x, nx^k, p^m)\right| \leq Dp^{m/2}, \tag{4.3}$$

when p is odd, and

$$\left|S_1(\chi, x, nx^k, p^m)\right| \leq (2,k)D2^{\frac{m}{2}},$$

when $p = 2$, $m \geq 3$, where

$$D = \begin{cases} (k, \phi(p^m)), & \text{for } p \text{ odd}, \\ (k, 2^{m-2}), & \text{for } p = 2,\ m \geq 3. \end{cases}$$

By Lemma 2.3.1 S_1 is zero unless $\chi = \chi_1^k$ for some character χ_1 mod p^m, thus we can write

$$\begin{aligned} S_1 &= \sum_{x=1}^{p^m} \chi(x) e_{p^m}\left(nx^k\right) = \sum_{x=1}^{p^m} \chi_1^k(x) e_{p^m}(nx^k) \\ &= \sum_{x=1}^{p^m} \chi_1(x^k) e_{p^m}(nx^k), \end{aligned}$$

and by Lemma 2.6.2 and Lemma 2.6.1,

$$S_1 = \sum_{\chi_2^D=\chi_0} \sum_{u=1}^{p^m} \chi_1\chi_2(u)e_{p^m}(nu) = \sum_{\chi_2^D=\chi_0} \sum_{u=1}^{p^m} \overline{\chi_1\chi_2}(n)\chi_1\chi_2(u)e_{p^m}(u)$$
$$= \sum_{\chi_2^D=\chi_0} \overline{\chi_1\chi_2}(n)G(\chi_1\chi_2, p^m).$$

When p is odd, there are $D = (k, \phi(p^m))$ characters χ_2 where $\chi_2^D = \chi_0$, and so one immediately obtains a Weil type bound

$$\left|S(\chi, x, nx^k, p^m)\right| \leq Dp^{m/2}. \tag{4.4}$$

When $p = 2$, $m \geq 3$ an additional factor of $(2, k)$ is needed by the fact that there are $(2, k)D$ characters with $\chi_2^D = \chi_0$.

4.3 Binomial Character Sums as Gauss Sums

In this section we write the binomial characters sum

$$S_2 = S_2(\chi_1, \chi_2, Ax^k + B) = \sum_{x=1}^{p^m} \chi_1(x)\chi_2(Ax^k + B)$$

in terms of Gauss sums. From Lemma 2.3.1 we know that this sum is zero unless $\chi_1 = \chi_3^k$ for some character χ_3 mod p^m, in which case the sum can be written as a sum of $(k, \phi(p^m))$ mod p^m Jacobi like sums $\sum_{x=1}^{p^m} \chi_5(x)\chi_2(Ax + B)$ and again be expressed in terms of Gauss sums.

Theorem 4.3.1. *Let p be an odd prime. If χ_1, χ_2 are characters mod p^m with χ_2 primitive and $\chi_1 = \chi_3^k$ for some character χ_3 mod p^m, $A, B \in \mathbb{Z}$ with $p \nmid B$ and n and A' are given by*

$$A = p^n A', \quad 0 \leq n < m, \quad p \nmid A', \tag{4.5}$$

then

$$\sum_{x=1}^{p^m} \chi_1(x)\chi_2(Ax^k+B) = p^n \sum_{\chi_4 \in X} \overline{\chi_3\chi_4}(A')\chi_2\chi_3\chi_4(B)\frac{G(\chi_3\chi_4, p^{m-n})G(\overline{\chi_2\chi_3\chi_4}, p^m)}{G(\overline{\chi_2}, p^m)}, \quad (4.6)$$

where X denotes the mod p^m characters χ_4 with $\chi_4^D = \chi_0$, $D = (k, \phi(p^m))$, such that $\chi_3\chi_4$ is a mod p^{m-n} character.

We immediately obtain the Weil type bound

$$\left|S(\chi_1, \chi_2, Ax^k + B, p^m)\right| \leq (k, \phi(p^m))p^{(m+n)/2}. \quad (4.7)$$

Before proving the Theorem 4.3.1 we note a number of special cases. For $m = 1$ and $p \nmid A$ this gives us the bound

$$\left|\sum_{x=1}^{p-1} \chi\left(x^l(Ax^k+B)^w\right)\right| \leq dp^{\frac{1}{2}},$$

where

$$d = (k, p-1). \quad (4.8)$$

For $l = 0$ we can slightly improve this for the complete sum,

$$\left|\sum_{x=0}^{p-1} \chi(Ax^k+B)\right| \leq (d-1)p^{\frac{1}{2}}, \quad (4.9)$$

since, taking $\chi_1 = \chi_3 = \chi_0$, $\chi_2 = \chi$, the $\chi_4 = \chi_0$ term in Theorem 4.3.1 equals $-\chi(B)$, the missing $x = 0$ term in (4.9). These correspond to the classical Weil bound (4.1) after an appropriate change of variables to replace k by d. For $m \geq t+1$ the bound (4.7) is $dp^{\frac{m+n}{2}+t}$, as we shall see in (6.12) we have equality in (4.7) for $m \geq n+2t+2$, but not for $t+n+1 < m < 2t+n+2$.

Notice that if $(k, \phi(p^m)) = 1$ and $\chi_1 = \chi_3^k$ and, in case $p \mid A$ for some mod p^{m-n} character,

χ_3, then we have the single $\chi_4 = \chi_0$ term and

$$\sum_{x=1}^{p^m} \chi_1(x)\chi_2(Ax^k + B) = p^n \overline{\chi}_3(A')\chi_2\chi_3(B)\frac{G(\chi_3, p^{m-n})G(\overline{\chi_2\chi_3}, p^m)}{G(\overline{\chi_2}, p^m)}.$$

Thus $\left|\sum_{x=1}^{p^m} \chi_1(x)\chi_2(Ax^k + B)\right| = p^{(m+n)/2}$ if $\chi_2, \chi_2\chi_3$ and χ_3 are primitive mod p^m and p^{m-n}. Noting that $\overline{G(\overline{\chi}, p^m)} = \chi(-1)G(\chi, p^m)$ this can be written $G(\chi_3, p^{m-n})G_2(\chi_2, p^m)/G(\chi_2\chi_3, p^m)$ and we plainly recover the form

$$J(\chi_1, \chi_2, p^m) = \frac{G(\chi_1, p^m)G(\chi_2, p^m)}{G(\chi_1\chi_2, p^m)} \tag{4.10}$$

in that case.

For the multiplicative analogue of the classical Kloostermann sum, χ assumed primitive and $p \nmid A$, Theorem 4.3.1 gives a sum of two terms of size $p^{m/2}$,

$$\sum_{x=1}^{p^m}{}^{*} \chi(Ax + x^{-1}) = \frac{\overline{\chi}_3(A)}{G(\overline{\chi}, p^m)}\left(G(\chi_3, p^m)^2 + \chi_Q(A)G\left(\chi_3\chi_Q, p^m\right)^2\right)$$

when $\chi = \overline{\chi}_3^2$ (otherwise the sum is zero), where χ_Q here denotes the mod p^m extension of the Legendre symbol (taking $\chi_2 = \chi$, $\chi_1 = \overline{\chi}$, $k = 2$ we have $D = 2$ and $\chi_4 = \chi_0$ or χ_Q). For $m = 1$ this is Han Di's [10, Lemma 1]. Cases where we can write the exponential sum explicitly in terms of Gauss sums are rare. Best known (after the quadratic Gauss sums) are perhaps the Salié sums, evaluated by Salié [25] for $m = 1$ (see Williams [27],[28] or Mordell [17] for a short proof) and Cochrane & Zheng [7, §5] for $m \geq 2$; for $p \nmid AB$

$$\sum_{x=1}^{p^m}{}^{*} \chi_Q(x)e_{p^m}(Ax + Bx^{-1}) = \chi_Q(B)\begin{cases} p^{\frac{1}{2}(m-1)}(e_{p^m}(2\gamma) + e_{p^m}(-2\gamma))G\left(\chi_Q, p\right), & m \text{ odd}, \\ p^{\frac{1}{2}m}\left(\chi_Q(\gamma)e_{p^m}(2\gamma) + \chi_Q(-\gamma)e_{p^m}(-2\gamma)\right), & m \text{ even}, \end{cases}$$

if $AB = \gamma^2 \bmod p^m$, and zero if $\chi_Q(AB) = -1$. Cochrane & Zheng's $m \geq 2$ method works

with a general χ as long as their critical point quadratic congruence does not have a repeated root, but formulae seem lacking when $m = 1$ and $\chi \neq \chi_Q$.

For the Jacobsthal sums we get (essentially Theorems 6.1.14 & 6.1.15 of [2])

$$\sum_{m=1}^{p-1} \left(\frac{m}{p}\right)\left(\frac{m^k+B}{p}\right) = \left(\frac{B}{p}\right)\sum_{j=0}^{k-1} \chi(B)^{2j+1}\frac{G(\chi^{2j+1},p)G(\overline{\chi}^{2j+1}\chi^*,p)}{G(\chi^*,p)},$$
$$\sum_{m=0}^{p-1} \left(\frac{m^k+B}{p}\right) = \left(\frac{B}{p}\right)\sum_{j=1}^{k-1} \chi(B)^{2j}\frac{G(\chi^{2j},p)G(\overline{\chi}^{2j}\chi^*,p)}{G(\chi^*,p)},$$

when $p \equiv 1 \bmod 2k$ and $p \nmid B$, where χ denotes a mod p character of order $2k$ (see also [13]).

Proof of Theorem 4.3.1. Observe that if χ is a primitive character mod p^j, $j \geq 1$, then by the duality Lemma 2.6.2,

$$\sum_{y=1}^{p^j} \chi(y)e_{p^j}(Ay) = \overline{\chi}(A)G(\chi,p^j). \tag{4.11}$$

Hence if χ_2 is a primitive character mod p^m we have

$$G(\overline{\chi_2},p^m)\chi_2(Ax^k+B) = \sum_{y=1}^{p^m} \overline{\chi_2}(y)e_{p^m}((Ax^k+B)y),$$

and, since $\chi_1 = \chi_3^k$ and $D = (k,\phi(p^m))$,

$$\begin{aligned} G(\overline{\chi_2},p^m)\sum_{x=1}^{p^m}\chi_1(x)\chi_2(Ax^k+B) &= \sum_{x=1}^{p^m}\chi_3(x^k)\sum_{y=1}^{p^m}\overline{\chi_2}(y)e_{p^m}((Ax^k+B)y) \\ &= \sum_{x=1}^{p^m}\chi_3(x^D)\sum_{y=1}^{p^m}\overline{\chi_2}(y)e_{p^m}((Ax^D+B)y). \end{aligned}$$

By Lemma 2.6.1 we have

$$\begin{aligned} G(\overline{\chi_2}, p^m)\sum_{x=1}^{p^m}\chi_1(x)\chi_2(Ax^k+B) &= \sum_{\chi_4^D=\chi_0}\sum_{u=1}^{p^m}\chi_3(u)\chi_4(u)\sum_{y=1}^{p^m}\overline{\chi_2}(y)e_{p^m}((Au+B)y) \\ &= \sum_{\chi_4^D=\chi_0}\sum_{y=1}^{p^m}\overline{\chi_2}(y)e_{p^m}(By)\sum_{u=1}^{p^m}\chi_3\chi_4(u)e_{p^m}(Auy) \\ &= \sum_{\chi_4^D=\chi_0}\sum_{y=1}^{p^m}\overline{\chi_2\chi_3\chi_4}(y)e_{p^m}(By)\sum_{u=1}^{p^m}\chi_3\chi_4(u)e_{p^m}(Au). \end{aligned}$$

Since $p\nmid B$ we have

$$\sum_{y=1}^{p^m}\overline{\chi_2\chi_3\chi_4}(y)e_{p^m}(By) = \chi_2\chi_3\chi_4(B)G(\overline{\chi_2\chi_3\chi_4}, p^m).$$

If $\chi_3\chi_4$ is a mod p^{m-n} character then

$$\sum_{u=1}^{p^m}\chi_3\chi_4(u)e_{p^m}(Au) = p^n\sum_{u=1}^{p^{m-n}}\chi_3\chi_4(u)e_{p^{m-n}}(A'u) = p^n\overline{\chi_3\chi_4}(A')G(\chi_3\chi_4, p^{m-n}).$$

If $\chi_3\chi_4$ is a primitive character mod p^j for some $m-n<j\le m$ then by Lemma 2.6.2

$$\sum_{u=1}^{p^m}\chi_3\chi_4(u)e_{p^m}(Au) = p^{m-j}\sum_{u=1}^{p^j}\chi_3\chi_4(u)e_{p^j}(p^{j-(m-n)}A'u) = 0,$$

and the result follows. □

Notice that if $m\ge n+2$ then by (4.2) the set X can be further restricted to those χ_4 with $\chi_3\chi_4$ primitive mod p^{m-n}. Hence if $p^t||\,k$, with $m\ge n+t+2$ and we write $\chi_3(a)=e_{\phi(p^m)}(c_3)$, $\chi_4(a)=e_{\phi(p^m)}(c_4)$ we have $p^{m-1-t}\mid c_4$, $p^n||\,(c_3+c_4)$, giving $p^n||\,c_3$. Letting $\chi_1=\chi^l=\chi_3^k$, for some mod p^m character, χ, this yields $p^{n+t}||\,c_3k=c_1=cl$ and $p^{n+t}||\,l$. If $n>0$, letting $\chi_2=\chi^w$, we deduce that $p^t||\,l+wk$. Moreover when $n=0$ reversing the roles of A and B

gives $p^t || \, l + wk$. Hence when $m \geq n + t + 2$ we have $S(\chi_1, \chi_2, Ax^k + B, p^m) = 0$ unless

$$p^{n+t} \, || \, l, \quad p^t \, || \, l + wk, \tag{4.12}$$

holds. For $m = n + t + 1$ we similarly still have $p^{n+t} \mid l$.

4.4 The Generalized Jacobi Sum as Gauss Sums

Finally we show that the generalized Jacobi sum

$$J_{p^n}(\chi_1, \ldots, \chi_k, p^m) = \sum_{x_1=1}^{p^m} \cdots \sum_{\substack{x_k=1 \\ x_1+\cdots+x_k=p^n}}^{p^m} \chi_1(x_1) \cdots \chi_k(x_k), \quad m > n \tag{4.13}$$

can be expressed in terms of Gauss sums, a fact that will be central in our proof of Theorem 7.0.1.

It is well known that the classical mod p Jacobi sums,

$$J(\chi_1, \chi_2, p) = \sum_{x=1}^{p} \chi_1(x)\chi_2(1-x), \tag{4.14}$$

(and their generalization to finite fields) can be written in terms of Gauss sums (see for example Theorem 2.1.3 of [2] or Theorem 5.21 of [14]). This extends to the mod p^m sums. For example when χ_1, χ_2 and $\chi_1\chi_2$ are primitive mod p^m

$$J(\chi_1, \chi_2, p^m) = \frac{G(\chi_1, p^m)G(\chi_2, p^m)}{G(\chi_1\chi_2, p^m)}, \tag{4.15}$$

and $|J(\chi_1, \chi_2, p^m)| = p^{m/2}$ (see Lemma 1 of [31] or [32]; the relationship for Jacobi sums over more general residue rings modulo prime powers can be found in [33]). Writing (4.15) in terms of Gauss sums is well known for the mod p sums and the corresponding result for (4.13) when $n = 0$ can be found, along with many other properties of Jacobi sums, in Berndt,

R. J. Evans and K. S. Williams [2, Theorem 2.1.3 & Theorem 10.3.1] or Lidl-Niederreiter [14, Theorem 5.21]. There the results are stated for sums over finite fields, $\mathbb{F}_{p^m}$, so it is not surprising that such expressions exist in the less studied mod p^m case. When $\chi_1, \ldots, \chi_k$ and $\chi_1 \cdots \chi_k$ are primitive, Zhang & Yao [30, Lemma 3] for $k = 2$, and Zhang and Xu [32, Lemma 1] for general k, showed that

$$J(\chi_1, \ldots, \chi_k, p^m) = \frac{\prod_{i=1}^{k} G(\chi_i, p^m)}{G(\chi_1 \cdots \chi_k, p^m)}. \tag{4.16}$$

In Theorem 4.4.1 we obtain a similar expansion for $J_{p^n}(\chi_1, \ldots, \chi_k, p^m)$, with $m > n$. As we showed in Theorem 3.1.1 the mod p^m Gauss sums can be evaluated explicitly using the method of Cochrane and Zheng [4] when $m \geq 2$. We shall need the counterpart of (4.16) for the $J_{p^n}(\chi_1, \ldots, \chi_k, p^m)$ along with the evaluation of the Gauss sum from Chapter 3 in order to evaluate $J_{p^n}(\chi_1, \ldots, \chi_k, p^m)$. We state a less symmetrical version to allow weaker assumptions on the χ_i:

Theorem 4.4.1. *Suppose that $\chi_1, \ldots, \chi_k$ are characters mod p^m with $m > n$ and χ_k primitive mod p^m. If $\chi_1 \cdots \chi_k$ is a mod p^{m-n} character, then*

$$J_{p^n}(\chi_1, \ldots, \chi_k, p^m) = p^n \frac{\overline{G(\chi_1 \cdots \chi_k, p^{m-n})}}{\overline{G(\chi_k, p^m)}} \prod_{i=1}^{k-1} G(\chi_i, p^m). \tag{4.17}$$

If $\chi_1 \cdots \chi_k$ is not a mod p^{m-n} character, then $J_{p^n}(\chi_1, \ldots, \chi_k, p^m) = 0$.

From the well known property of Gauss sums (see for example Section 1.6 of [2]),

$$|\, G(\chi, p^j) \,| = \begin{cases} p^{j/2}, & \text{if } \chi \text{ is primitive mod } p^j, \\ 1, & \text{if } \chi = \chi_0 \text{ and } j = 1, \\ 0, & \text{otherwise,} \end{cases} \tag{4.18}$$

when $\chi_1 \cdots \chi_k$ is a primitive mod p^{m-n} character and at least one of the χ_i is a primitive

mod p^m character, we immediately obtain the symmetric form

$$J_{p^n}(\chi_1,\dots,\chi_k,p^m)=\frac{\prod_{i=1}^k G(\chi_i,p^m)}{G(\chi_1\cdots\chi_k,p^{m-n})}. \tag{4.19}$$

In particular we recover (4.16) under the sole assumption that $\chi_1\cdots\chi_k$ is a primitive mod p^m character.

Proof. We first note that if χ is a primitive character mod p^j, $j\geq 1$, then by Lemma 2.6.2

$$\sum_{y=1}^{p^j}\chi(y)e_{p^j}(Ay)=\overline{\chi}(A)G(\chi,p^j).$$

Hence if χ_k is a primitive character mod p^m we have

$$\begin{aligned}
&\overline{\chi}_k(-1)G(\overline{\chi}_k,p^m)\sum_{x_1=1}^{p^m}\cdots\sum_{x_{k-1}=1}^{p^m}\chi_1(x_1)\dots\chi_{k-1}(x_{k-1})\chi_k(p^n-x_1-\cdots-x_{k-1})\\
&=\overline{\chi}_k(-1)\sum_{x_1=1}^{p^m}\cdots\sum_{x_{k-1}=1}^{p^m}\chi_1(x_1)\dots\chi_{k-1}(x_{k-1})\sum_{y=1}^{p^m}\overline{\chi}_k(y)e_{p^m}((p^n-x_1-\cdots-x_{k-1})y)\\
&=\sum_{\substack{y=1\\ p\nmid y}}^{p^m}\overline{\chi}_k(-y)e_{p^m}(p^ny)\left(\sum_{x_1=1}^{p^m}\chi_1(x_1)e_{p^m}(-x_1y)\cdots\sum_{x_{k-1}=1}^{p^m}\chi_{k-1}(x_{k-1})e_{p^m}(-x_{k-1}y)\right)\\
&=\sum_{\substack{y=1\\ p\nmid y}}^{p^m}\overline{\chi_1\cdots\chi_k}(-y)e_{p^m}(p^ny)\left(\sum_{x_1=1}^{p^m}\chi_1(x_1)e_{p^m}(x_1)\cdots\sum_{x_{k-1}=1}^{p^m}\chi_{k-1}(x_{k-1})e_{p^m}(x_{k-1})\right)\\
&=\overline{\chi_1\cdots\chi_k}(-1)\sum_{\substack{y=1\\ p\nmid y}}^{p^m}\overline{\chi_1\cdots\chi_k}(y)e_{p^m}(p^ny)\prod_{i=1}^{k-1}G(\chi_i,p^m).
\end{aligned}$$

If $m>n$ and $\overline{\chi_1\cdots\chi_k}$ is a mod p^{m-n} character, then

$$\sum_{\substack{y=1\\ p\nmid y}}^{p^m}\overline{\chi_1\cdots\chi_k}(y)e_{p^m}(p^ny)=p^n\sum_{\substack{y=1\\ p\nmid y}}^{p^{m-n}}\overline{\chi_1\cdots\chi_k}(y)e_{p^{m-n}}(y)=p^nG(\overline{\chi_1\cdots\chi_k},p^{m-n}).$$

If $\overline{\chi_1 \dots \chi_k}$ is a primitive character mod p^j with $m-n < j \leq m$, then by the same reasoning as in Lemma 2.6.2

$$\sum_{\substack{y=1 \\ p \nmid y}}^{p^m} \overline{\chi_1 \cdots \chi_k}(y) e_{p^m}(p^n y) = p^{m-j} \sum_{y=1}^{p^j} \overline{\chi_1 \cdots \chi_k}(y) e_{p^j}(p^{j-(m-n)} y)) = 0,$$

and the result follows on observing that

$$\overline{G(\chi, p^m)} = \overline{\chi}(-1) G(\overline{\chi}, p^m).$$

□

Chapter 5

Evaluating the Twisted Monomial Sums Modulo Prime Powers

We use the Cochrane and Zheng reduction method to show that the sum

$$S_1(\chi, nx^{\gamma p^t}, p^m) = \sum_{x=1}^{p^m} \chi(x) e_{p^m}(nx^{\gamma p^t})$$

has an explict evaluation for m sufficiently large.

For a multiplicative character χ mod q and $f(x) \in \mathbb{Z}[x]$ we define the twisted Gauss sum

$$S(\chi, f(x), q) := \sum_{x=1}^{q} \chi(x) e_q(f(x))$$

where $e_q(x) = e^{2\pi i x/q}$. We are concerned here with evaluating these sums when $f(x) = nx^k$ is a monomial and the modulus is a prime power $q = p^m$ with $m \geq 2$. Obtaining satisfactory bounds, other than the Weil bound [24], remains a difficult problem when $m = 1$ (see for example Heath-Brown and Konyagin [12]). For higher powers though, methods of Cochrane and Zheng [4] can often be used to reduce the modulus of an exponential sum and sometimes evaluate the sum exactly.

When the modulus q is squarefull, i.e. $p \mid q \Rightarrow p^2 \mid q$, and $(2nk, q) = 1$, Zhang and Liu [37] consider the fourth power mean value of $|S(\chi, nx^k, q)|$, averaged over the characters χ mod q, and obtained

$$\sum_{\chi \bmod q} \left|S(\chi, nx^k, q)\right|^4 = q\phi^2(q) \prod_{p|q} (k, p-1)^2, \tag{5.1}$$

(their formula contains an additional factor when there are primes $p \mid q$ with $(k, p-1) = 1$ due to an apparent miscount in their Lemma 5). In the quadratic case, $|S(\chi, nx^2, q)|$, He and Zhang [29] obtain similar exact expressions for the sixth and eighth power means when q is squarefull and coprime to $2n$, making the conjecture, subsequently proved by Liu and Yang [34], that

$$\sum_{\chi \bmod q} |S(\chi, nx^2, q)|^{2\ell} = 4^{(\ell-1)\omega(q)} q^{\ell-1} \phi^2(q), \qquad \omega(q) := \sum_{p|q} 1, \tag{5.2}$$

for any integer $\ell \geq 2$. Similarly Guo Xiaoyan and Wang Tingting [26] consider power means averaged over the parameter n for quadratic and cubic sums, again q squarefull with $(2n, q) = 1$ and $(6n, q) = 1$ respectively, showing that for any real $\ell \geq 0$,

$$\sum_{\substack{n=1 \\ (n,q)=1}}^{q} |S(\chi, nx^2, q)|^{2\ell} = 2^{(2\ell-1)\omega(q)} q^{\ell} \phi(q), \tag{5.3}$$

when χ is the square of a primitive character mod q (and zero otherwise), and

$$\sum_{\substack{n=1 \\ (n,q)=1}}^{q} |S(\chi, nx^3, q)|^4 = 27^{\omega_1(q)} q^2 \phi(q), \qquad \omega_1(q) := \sum_{\substack{p|q \\ 3|p-1}} 1, \tag{5.4}$$

when χ is the cube of a primitive character mod q (and zero otherwise). These average results all generalize to arbitrary monomials nx^k and arbitrary real power means as we show in Corollary 5.0.1 below.

Actually, the methods in Cochrane and Zheng [4] can be used to evaluate the individual sums $S(\chi, nx^k, p^m)$ directly when $m \geq 2$, $(p, 2nk) = 1$, with no need to average.

Moreover (due to the straightforward relationship between the α satisfying (2.27)) for general $f(x) = nx^k$, $(2nk, p) = 1$, $m \geq 2$, the $\sum S_\alpha$ arising in Cochrane and Zheng's method will, with a little work, simplify down to a single term of modulus $(k, p-1)p^{m/2}$. A fact that is just a special case of our main Theorem of this chapter, Theorem 5.1.1. When $p \mid k$, though, the critical points are multiple roots so one has to do more work. However we show here that Cochrane and Zheng's method can be adjusted to deal with the case $p \mid k$. Additionally our approach reduces to finding a single solution of a certain *characteristic equation* (5.13) or (5.14), avoiding the need to sum as with the original S_α.

Working mod p^m we write

$$f(x) = nx^{\gamma p^t}, \qquad p \nmid \gamma n, \tag{5.5}$$

and define

$$d = (\gamma, p-1). \tag{5.6}$$

Analogous to the squarefull condition in [26], [29], [34] and [37] we shall assume that

$$m \geq t + 2. \tag{5.7}$$

Theorem 5.0.2. *Let p be an odd prime, χ be a character mod p^m and suppose that (5.5) and (5.7) hold.*

If χ is the dp^t-th power of a primitive character mod p^m and an appropriate characteristic equation (5.13) or (5.14) has a solution then

$$\left| S_1(\chi, nx^{\gamma p^t}, p^m) \right| = dp^\tau$$

where

$$\tau = \begin{cases} m-1, & \text{if } t+1 < m \le 2t+2, \\ \frac{m}{2}+t, & \text{if } 2t+2 \le m. \end{cases} \tag{5.8}$$

Otherwise $S_1(\chi, nx^{\gamma p^t}, p^m) = 0$.

Theorem 5.0.2 is an immediate consequence of our main Theorem (5.1.1), where we state an explicit formula for $S_1(\chi, nx^{\gamma p^t}, p^m)$. The corresponding result for $p = 2$ is given in (5.34). Averaging over the n or χ we immediately obtain:

Corollary 5.0.1. *Under the same hypotheses of Theorem 5.0.2, for any real* $b > 0$,

$$\sum_{\chi \bmod p^m} |S_1(\chi, nx^{\gamma p^t}, p^m)|^b = (dp^\tau)^b \frac{\phi^2(p)}{d^2} p^{\max\{m-2t-2,0\}}, \tag{5.9}$$

and when χ *is a* dp^t*-th power of a primitive character mod* p^m,

$$\sum_{\substack{n=1 \\ (n,p)=1}}^{p^m} |S_1(\chi, nx^{\gamma p^t}, p^m)|^b = (dp^\tau)^b \frac{\phi(p)}{d} p^{\max\{m-t-1,\, t+1\}}. \tag{5.10}$$

The corresponding results for composite moduli (including (5.1–5.4)) then follow immediately from the multiplicativity discussed in Section 2.2. Since Theorem 5.0.2 shows that the $|S_1(\chi, nx^{\gamma p^t}, p^m)|$ can assume only one nonzero value, power means are somewhat artificial here, with (5.9) and (5.10) amounting only to a count on the number of non-zero cases (we include them for comparison with results in the literature and to emphasize that the restriction to certain integer power means is unnecessary).

The condition (5.7) is appropriate here. For $t \ge m$ the exponent reduces by Euler's Theorem and as shown in the proof of Theorem 2.1 (see (5.22)) when $m = t+1$ the sum is zero unless χ is a mod p character, in which case it reduces to a Heilbronn type mod p sum

$$S(\chi, nx^{\gamma p^{m-1}}, p^m) = p^{m-1} \sum_{x=1}^{p-1} \chi(x) e_{p^m}(nx^{\gamma p^{m-1}}).$$

For $m = 2$ and $d = 1$ these are the classical Heilbronn sums, bounded using the Stepanov method by Heath-Brown [11] and Heath-Brown and Konyagin [12], extended by Puchta [23] and improved by Malykhin [35] to deal with $d = (\gamma, p-1) > 1$, the latter estimate being

$$\left|\sum_{x=1}^{p-1} e_{p^2}(nx^{\gamma p})\right| \ll d^{1/2}\, p^{7/8}.$$

We note that although not stated in their theorems, their methods would allow the inclusion of a mod p character χ. Obtaining exact values seems unlikely for these types of sum. In [36] Malykhin considers the general case $m > 2$, obtaining

$$\left|\sum_{x=1}^{p-1} e_{p^m}\left(nx^{p^{m-1}}\right)\right| \leq C(m)p^{1-1/32\cdot 5^{m-3}}.$$

We have assumed here that $p \nmid n$. If $p \mid n$ and χ is a primitive character mod p^m then $S_1(\chi, nx^{\gamma p^t}, p^m) = 0$ as can be seen from the proof of Theorem 5.1.1 (if $p \mid n$ and $p \nmid c$ then the characteristic equation (5.19) or (5.24) will have no solution). If $p \mid n$ and χ is a mod p^{m-1} character then plainly we can reduce to a mod p^{m-1} sum.

5.1 Statement of the Main Theorem

Suppose that p is an odd prime and a is a primitive root mod p^l for all l. Recall we define the integers R_l, $p \nmid R_l$, by

$$a^{\phi(p^l)} = 1 + R_l p^l, \tag{5.11}$$

and the integers r and c by

$$r := R_1, \qquad \chi(a) = e\left(c/\phi(p^m)\right). \tag{5.12}$$

Note that χ is a primitive character mod p^m if and only if $p \nmid c$.

We first observe that $S_1(\chi, nx^{\gamma p^t}, p^m) = 0$ if χ is not a dp^t-th power of a character where $d = (\gamma, p-1)$, by Lemma 2.3.1. An alternative proof of this result will occur during the proof of Theorem 2.1 below.

If χ is the dp^tth power of a character χ_1 and c_1 an integer such that

$$\chi_1(a) = e\left(c_1/\phi(p^m)\right)$$

then as we shall see, the final characteristic equation for the evaluation of S_1 will take one of the two following forms (depending on the size of t relative to m).

Case I: When $t+1 < m \leq 2t+2$

$$c_1 + R_{t+1} n x^{\gamma p^t} \equiv 0 \mod p^{m-t-1}. \tag{5.13}$$

Case II: When $2t+2 < m$

$$c_1 + R_{t+s+1} n x^{\gamma p^t} \equiv 0 \mod p^{t+s+1}, \tag{5.14}$$

where

$$s := \max\left\{0, \left\lceil \frac{m}{3} \right\rceil - t - 1\right\}.$$

Expressions simplify slightly in Case II if we use the stronger congruence

$$c_1 + R_{\lceil \frac{m}{2} \rceil} n x^{\gamma p^t} \equiv 0 \mod p^{\lceil \frac{m}{2} \rceil}, \tag{5.15}$$

except for $p = 3$, $m = 3$, $t = 0$ when we need $c_1 + R_{\lceil \frac{m}{2} \rceil} n x^{\gamma} \equiv -3c_1 R_{t+s+1}^2 \mod 9$.

Notice that, since x^k and $x^{(k,\phi(p^m))}$ run through the same set of values mod p^m,

$$S(\chi_1^k, nx^k, p^m) = S(\chi_1^{(k,\phi(p^m))}, nx^{(k,\phi(p^m))}, p^m), \tag{5.16}$$

and so one can always reduce to a monomial nx^{dp^t} with $d \mid p-1$, though we shall not assume this here.

Theorem 5.1.1. *For p an odd prime, $t \in \mathbb{Z}$, $t \geq 0$, let*

$$f(x) = nx^{\gamma p^t}, \quad p \nmid n\gamma.$$

Case I: Suppose that $t+1 < m \leq 2t+2$. If χ is a dp^t-th power of a primitive character and the characteristic equation (5.13) has a solution α then

$$S_1(\chi, f(x), p^m) = dp^{m-1}\chi(\alpha)e_{p^m}(f(\alpha)).$$

Otherwise, $S_1(\chi, f(x), p^m) = 0$.

Case II: Suppose that $2t+2 < m$. If χ is a dp^t-th power power of a primitive character and (5.14) has a solution then

$$S_1(\chi, f(x), p^m) = dp^{\frac{m}{2}+t}\chi(\alpha)e_{p^m}(f(\alpha))\left(\frac{-2rc_1}{p^m}\right)\varepsilon_{p^m}, \tag{5.17}$$

where α is a solution of (5.15), and r and ε_{p^m} are as in (2.8) and (2.29). Otherwise $S_1(\chi, f(x), p^m) = 0$.

Note in Case II we can use a solution α to the weaker congruence (5.14) if we include in (5.17) an additional factor

$$e_{p^{m-2t-2s-2}}(-2^{-2}\beta_1^{-1}\beta_2^2) \tag{5.18}$$

where, writing $c_1 + R_{t+s+1}n\alpha^{\gamma p^t} = \lambda_1 p^{t+s+1}$, $\beta_1 := -2^{-1}R_{t+s+1}c_1$, $\beta_2 := \lambda_1 - \beta_1$. Here and throughout x^{-1} denotes the multiplicative inverse of x mod p^m.

5.2 Proof of Theorem 5.1.1

We start by rewriting the sum in terms of our primitive root a

$$S_1(\chi, nx^{\gamma p^t}, p^m) = \sum_{\substack{x=1 \\ p\nmid x}}^{p^m} \chi(x) e_{p^m}(nx^{\gamma p^t}) = \sum_{k=1}^{\phi(p^m)} \chi(a^k) e_{p^m}(na^{k\gamma p^t}).$$

We set $\gamma = d\gamma'$, where recall $d = (\gamma, p-1)$, and let c be an integer such that

$$\chi(a) = e\left(\frac{c}{\phi(p^m)}\right) = e\left(\frac{c}{p^{m-1}(p-1)}\right).$$

Case I: Suppose that $t+1 < m \leq 2t+2$.

We let $u = 1, ..., dp^{m-1}$ and let v run through an interval I of $\frac{p-1}{d}$ consecutive integers so that $k = u\frac{p-1}{d} + v$ sums over $\phi(p^m)$ consecutive integers and

$$\sum_{k=1}^{\phi(p^m)} \chi(a^k) e_{p^m}(na^{k\gamma p^t}) = \sum_{v\in I} \sum_{u=1}^{dp^{m-1}} \chi(a^{u\frac{p-1}{d}+v}) e_{p^m}(na^{(u\frac{p-1}{d}+v)\gamma p^t})$$

$$= \sum_{v\in I} \chi(a^v) e_{p^m}(na^{\gamma p^t v}) \sum_{u=1}^{dp^{m-1}} e\left(\frac{cu}{dp^{m-1}}\right) e_{p^m}\left(na^{\gamma p^t v}\left(a^{p^t(p-1)\gamma' u} - 1\right)\right).$$

Since $2(t+1) \geq m$ the binomial expansion gives

$$a^{p^t(p-1)\gamma' u} - 1 = (1 + R_{t+1}p^{t+1})^{\gamma' u} - 1 \equiv \gamma' u R_{t+1} p^{t+1} \bmod p^m,$$

and the inner sum becomes

$$\sum_{u=1}^{dp^{m-1}} e\left(\frac{u(c + R_{t+1}p^t\gamma n a^{\gamma p^t v})}{dp^{m-1}}\right) = dp^{m-1},$$

if v satisfies

$$c + R_{t+1}p^t\gamma n a^{\gamma p^t v} \equiv 0 \bmod dp^{m-1}, \tag{5.19}$$

and zero otherwise. We must examine when (5.19) has solutions.

Since $d \mid R_{t+1}p^t\gamma n a^{\gamma p^t v}$, in order to have a solution we must have $d \mid c$. Similarly, since $p \nmid R_{t+1}\gamma n$ and $t < m-1$, we must have that $p^t || c$. So χ is a dp^tth power of a primitive character. Letting $c = c'p^t d$ and $\gamma = d\gamma'$ reduces our congruence to

$$c' + R_{t+1}\gamma' n a^{\gamma p^t v} \equiv 0 \bmod p^{m-t-1}. \tag{5.20}$$

Hence (5.20) has no solution and $S_1(\chi, nx^{\gamma p^t}, p^m) = 0$ if there is no solution to the characteristic equation

$$c' + R_{t+1}\gamma' n x^{\gamma p^t} \equiv 0 \bmod p^{m-t-1}. \tag{5.21}$$

If this equation has a solution $\alpha = a^{v_0}$ we take I to be an interval containing v_0. Solutions v to (5.20) must then satisfy $a^{\gamma p^t v} \equiv a^{\gamma p^t v_0} \bmod p^{m-t-1}$, that is $\gamma p^t v \equiv \gamma p^t v_0 \bmod p^{m-t-2}(p-1)$. Since $t \geq m-t-2$ this reduces to

$$v \equiv v_0 \bmod (p-1)/d,$$

and we have exactly the one solution $v = v_0$ in our range for v.

Hence

$$S_1(\chi, nx^{\gamma p^t}, p^m) = dp^{m-1}\chi(\alpha)e_{p^m}(f(\alpha)).$$

Writing $c \equiv \gamma p^t c_1 \bmod \phi(p^m)$ we have $c' \equiv c_1\gamma' \bmod p^{m-t-1}$ and so the characteristic equation (5.21) can be written equivalently in the form (5.13).

Note: If $m = t+1$ the same analysis gives $p^{m-1} \mid c$ and χ is a mod p character, and the sum reduces to

$$S_1(\chi, nx^{p^{m-1}\gamma}, p^m) = p^{m-1}\sum_{x=1}^{p}\chi(x)e_{p^m}(nx^{p^{m-1}\gamma}). \tag{5.22}$$

Case II: Suppose that $2t+2 < m$.

We now let $s = \max\{\lceil \frac{m}{3} \rceil - t - 1, 0\}$, $u = 1, ..., dp^{m-s-1}$ and let v run through an interval

I of $p^s(\frac{p-1}{d})$ consecutive integers where $d := (\gamma, p-1)$ as before. Letting $k = up^s(\frac{p-1}{d}) + v$ we are still summing over $\phi(p^m)$ consecutive terms and

$$\sum_{k=1}^{\phi(p^m)} \chi(a^k) e_{p^m}(na^{k\gamma p^t}) = \sum_{v\in I} \sum_{u=1}^{dp^{m-s-1}} \chi(a^{up^s(\frac{p-1}{d})+v}) e_{p^m}(na^{(up^s(\frac{p-1}{d})+v)\gamma p^t})$$

$$= \sum_{v\in I} \chi(a^v) e_{p^m}(f(a^v)) \sum_{u=1}^{dp^{m-s-1}} e\left(\frac{cu}{dp^{m-1-s}}\right) e_{p^m}\left(na^{\gamma p^t v}\left(a^{p^{t+s}(p-1)\gamma' u} - 1\right)\right). \qquad (5.23)$$

Expanding binomially, observing that $3(t+s+1) \geq m$, we obtain

$$a^{p^{t+s}(p-1)\gamma' u} - 1 = \left(1 + R_{t+s+1}p^{t+s+1}\right)^{\gamma' u} - 1$$
$$\equiv u\gamma' R_{t+s+1}p^{t+s+1} + 2^{-1}u\gamma'(u\gamma' - 1)R_{t+s+1}^2 p^{2t+2s+2} \bmod p^m,$$

and the inner sum becomes

$$\sum_{u=1}^{dp^{m-s-1}} e\left(\frac{u\left(c + R_{t+s+1}\gamma n a^{\gamma p^t v} p^t + 2^{-1}\gamma R_{t+s+1}^2(u\gamma' - 1)n a^{\gamma p^t v} p^{2t+s+1}\right)}{dp^{m-s-1}}\right).$$

We now let $w = 1, ..., dp^{2t+s+1}$ and $y = 1, ..., p^{m-2t-2s-2}$, noting that $m - 2t - 2s - 2 \geq 0$ with equality only when $m = 4$, $t = 0$. Hence if $u = wp^{m-2t-2s-2} + y$ we again sum over dp^{m-s-1} consecutive integers and we can split the u sum as a product $S_1(v)S_2(v)$ of a y sum and a w sum, where

$$E_1(v) = \sum_{y=1}^{p^{m-2t-2s-2}} e\left(\frac{y\left(c + R_{t+s+1}\gamma n a^{\gamma p^t v} p^t + 2^{-1}\gamma R_{t+s+1}^2(y\gamma' - 1)n a^{\gamma p^t v} p^{2t+s+1}\right)}{dp^{m-s-1}}\right),$$

and

$$E_2(v) = \sum_{w=1}^{dp^{2t+s+1}} e\left(\frac{w\left(c + R_{t+s+1}\gamma n a^{\gamma p^t v} p^t\right)}{dp^{2t+s+1}}\right).$$

Now $E_2(v) = dp^{2t+s+1}$ if

$$c + \gamma R_{t+s+1} n a^{p^t \gamma v} p^t \equiv 0 \bmod dp^{2t+s+1}, \tag{5.24}$$

and $E_2(v) = 0$ otherwise. So again we must examine when (5.24) has solutions. Right away we see that in order to have a solution we must have $p^t || c$ and $d \mid c$, so our congruence reduces to

$$c' + \gamma' R_{t+s+1} n a^{p^t \gamma v} \equiv 0 \bmod p^{t+s+1} \tag{5.25}$$

where $c = c' dp^t$, $p \nmid c'$ and χ is a dp^tth power of a primitive character. Thus if the characteristic equation

$$c' + \gamma' R_{t+s+1} n x^{\gamma p^t} \equiv 0 \bmod p^{t+s+1} \tag{5.26}$$

has no solution we have $S_1(\chi, nx^{\gamma p^t}, p^m) = 0$. If it has a solution $\alpha = a^{v_0}$ we again choose I to be an interval containing v_0. Hence if v is a solution to (5.25) then $a^{\gamma p^t v} \equiv a^{\gamma p^t v_0} \bmod p^{t+s+1}$, that is $\gamma p^t v \equiv \gamma p^t v_0 \bmod p^{t+s}(p-1)$ reducing to

$$v \equiv v_0 \bmod p^s (p-1)/d.$$

So we have only the solution $v = v_0$ in I and so by (5.23)

$$\begin{aligned} S_1(\chi, nx^{\gamma p^t}, p^m) &= \chi(a^{v_0}) e_{p^m}(f(a^{v_0})) S_1(v_0) S_2(v_0) \\ &= dp^{2t+s+1} \chi(\alpha) e_{p^m}(f(\alpha)) S_1(v_0). \end{aligned} \tag{5.27}$$

When $m = 4$, $t = 0$, plainly $E_1(v_0) = 1$. Otherwise writing

$$c' + \gamma' R_{t+s+1} n a^{p^t \gamma v_0} = \lambda p^{t+s+1}, \quad \delta_1 := -2^{-1} R_{t+s+1} \gamma' c', \quad \delta_2 := \lambda + 2^{-1} R_{t+s+1} c',$$

observing that $3t + 2s + 2 \geq m - s - 1$ and that $y_1 = y + 2^{-1} \delta_1^{-1} \delta_2$ runs through a complete

set of residues mod $p^{m-2t-2s-2}$ as y does, we can rewrite $E_1(v_0)$ in terms of a classical, readily evaluated (see for example Apostol [1, §9.10 and Exercise 8.16] or Berndt, Evans and Williams [2, Theorem 1.5.2]), quadratic Gauss sum:

$$\begin{aligned} E_1(v_0) &= \sum_{y=1}^{p^{m-2t-2s-2}} e\left(\frac{y\left(\lambda - 2^{-1}R_{t+s+1}(y\gamma' - 1)c'\right)}{p^{m-2t-2s-2}}\right) \\ &= \sum_{y=1}^{p^{m-2t-2s-2}} e\left(\frac{\delta_1 y^2 + \delta_2 y}{p^{m-2t-2s-2}}\right) \\ &= e\left(-\frac{2^{-2}\delta_1^{-1}\delta_2^2}{p^{m-2t-2s-2}}\right) \sum_{y_1=1}^{p^{m-2t-2s-2}} e\left(\frac{\delta_1 y_1^2}{p^{m-2t-2s-2}}\right) \\ &= e\left(-\frac{2^{-2}\delta_1^{-1}\delta_2^2}{p^{m-2t-2s-2}}\right)\left(\frac{\delta_1}{p^m}\right) p^{\frac{m}{2}-t-s-1}\varepsilon_{p^m}, \end{aligned}$$

with ε_{p^m} as given in (2.29).

Thus by (5.27),

$$S_1(\chi, f(x), p^m) = dp^{\frac{m}{2}+t}\chi(\alpha)e_{p^m}(f(\alpha))e_{p^{m-2t-2s-2}}(-2^{-2}\delta_1^{-1}\delta_2^2)\left(\frac{\delta_1}{p^m}\right)\varepsilon_{p^m} \tag{5.28}$$

if χ is a dp^tth power power of a primitive character and $c' + \gamma' R_{t+s+1} n x^{p^t\gamma} \equiv 0 \bmod p^{t+s+1}$ has a solution α, and $S_1(\chi, f(x), p^m) = 0$ otherwise. Replacing $c' \equiv c_1\gamma' \bmod p^{m-t-1}$ we have $\lambda \equiv \lambda_1\gamma'$, $\delta_1 \equiv \beta_1\gamma'^2$, $\delta_2 \equiv \gamma'\beta_2 \bmod p^{m-t-1}$, with $\left(\frac{\delta_1}{p}\right) = \left(\frac{\beta_1}{p}\right) = \left(\frac{-2rc_1}{p}\right)$. Thus we obtain (5.17) with the additional factor (5.18). It remains to show that if we use a solution α to (5.14) satisfying the stronger congruence (5.15) then this additional factor is 1.

Plainly we can assume that $2(s+t+1) < m \le 3(s+t+1)$ and $\lceil \frac{m}{2} \rceil \le 2(s+t+1)$ with equality only when $s = t = 0$ and $m = 3$. We first note that

$$R_{\lceil \frac{m}{2} \rceil} \equiv R_{t+s+1} - 2^{-1}R_{t+s+1}^2 p^{s+t+1} + 3^{-1}R_{t+s+1}^3 p^{2(s+t+1)} \bmod p^{\lceil \frac{m}{2} \rceil},$$

where the last term vanishes unless $p = 3$, $m = 3$ and $t = 0$. To see this, observe that

$$\begin{aligned}
1 + R_{\lceil \frac{m}{2} \rceil} p^{\lceil \frac{m}{2} \rceil} &= \left(1 + R_{t+s+1} p^{s+t+1}\right)^{p^{\lceil \frac{m}{2} \rceil - s - t - 1}} \\
&\equiv 1 + R_{t+s+1} p^{\lceil \frac{m}{2} \rceil} + \frac{1}{2} R_{t+s+1}^2 p^{\lceil \frac{m}{2} \rceil + s + t + 1} \left(p^{\lceil \frac{m}{2} \rceil - s - t - 1} - 1\right) \\
&\quad + \frac{1}{6} R_{t+s+1}^3 p^{\lceil \frac{m}{2} \rceil + 2(s+t+1)} \left(p^{\lceil \frac{m}{2} \rceil - s - t - 1} - 1\right) \left(p^{\lceil \frac{m}{2} \rceil - s - t - 1} - 2\right) \mod p^{4(s+t+1)} \\
&\equiv 1 + p^{\lceil \frac{m}{2} \rceil} \left(R_{t+s+1} - 2^{-1} R_{t+s+1}^2 p^{s+t+1} + 3^{-1} R_{t+s+1}^3 p^{2(s+t+1)}\right) \mod p^{2\lceil \frac{m}{2} \rceil}.
\end{aligned}$$

In particular, $R_{\lceil \frac{m}{2} \rceil} \equiv R_{t+s+1} \mod p^{s+t+1}$. Hence if α is a solution to (5.14), which also satisfies (5.15),

$$c_1 + R_{t+s+1} n \alpha^{\gamma p^t} = \lambda_1 p^{s+t+1}, \quad c_1 + R_{\lceil \frac{m}{2} \rceil} n \alpha^{\gamma p^t} \equiv -c_1 3^{-1} R_{t+s+1}^2 p^{2(s+t+1)} \mod p^{\lceil \frac{m}{2} \rceil},$$

and so

$$c_1 (R_{\lceil \frac{m}{2} \rceil} - R_{t+s+1}) \equiv p^{s+t+1} \left(R_{t+s+1} \lambda_1 + c_1 3^{-1} R_{t+s+1}^3 p^{s+t+1}\right) \mod p^{\lceil \frac{m}{2} \rceil},$$

and

$$-2^{-1} c_1 R_{t+s+1} \equiv \lambda_1 \mod p^{\lceil \frac{m}{2} \rceil - s - t - 1}.$$

Hence $\beta_2 \equiv 0 \mod p^{\lceil \frac{m}{2} \rceil - s - t - 1}$ and $e_{p^{m-2t-2s-2}} \left(-2^{-2} \beta_1^{-1} \beta_2^2\right) = 1$.

Finally we need to verify that a solution a^{v_0} to (5.14) guarantees a solution a^v of (5.15). Since $R_{\lceil \frac{m}{2} \rceil} \equiv R_{t+s+1} \mod p^{s+t+1}$,

$$c_1 + R_{\lceil \frac{m}{2} \rceil} n a^{v_0 \gamma p^t} = \lambda p^{s+t+1}$$

for some integer λ. Taking $v = v_0 + h\phi\left(p^{s+1}\right)$ we have

$$\begin{aligned} c_1 + R_{\lceil \frac{m}{2} \rceil} n a^{v\gamma p^t} &= c_1 + R_{\lceil \frac{m}{2} \rceil} n a^{v_0 \gamma p^t} a^{h\gamma\phi\left(p^{s+t+1}\right)} \\ &= \lambda p^{s+t+1} + R_{\lceil \frac{m}{2} \rceil} n a^{v_0\gamma p^t} \left((1 + R_{t+s+1} p^{s+t+1})^{\gamma h} - 1\right) \\ &\equiv p^{s+t+1} \left(\lambda + R_{\lceil \frac{m}{2} \rceil} n a^{v_0 \gamma p^t} \gamma R_{t+s+1} h\right) \mod p^{2(s+t+1)}, \end{aligned}$$

and choosing h with $\lambda + R_{t+s+1}^2 n a^{v_0\gamma p^t}\gamma h \equiv -c_1 3^{-1} R_{t+s+1}^2 p^{s+t+1} \mod p^{\lceil \frac{m}{2} \rceil - s - t - 1}$ gives the required solution.

□

5.3 Proof of Corollary 5.0.1

From Theorem 2.1 we know that if $S_1(\chi, nx^{\gamma p^t}, p^m)$ is non zero then χ must be a dp^tth power of a primitive character mod p^m, and there must be a solution to a characteristic equation (5.21) or (5.26),

$$c' + r'\gamma' n x^{\gamma p^t} \equiv 0 \mod p^\kappa, \tag{5.29}$$

where $c = c' dp^t < \phi(p^m)$, $(nc', p) = 1$, and r' and κ depend on the range of t. If such is the case then $|S_1(\chi, nx^{\gamma p^t}, p^m)| = dp^\tau$. Thus to prove Corollary 1.1 we simply count the χ (i.e. count the c') or n that give us solutions. Writing in terms of our primitive root $x = a^v$, $-r'\gamma' n = a^{v_o}$, $c' = a^{v_1}$, (5.29) becomes,

$$(a^v)^{\gamma p^t} \equiv a^{v_1 - v_0} \mod p^\kappa,$$

which is equivalent to

$$\gamma p^t v \equiv v_1 - v_0 \mod \phi(p^\kappa).$$

This linear congruence in v has a solution when

$$(\gamma p^t, \phi(p^\kappa)) = d(p^t, p^{\kappa-1}) = dp^{\min\{m-t-2,t\}}$$

divides $v_1 - v_0$. So we have $\frac{\phi(p^\kappa)}{dp^{\min\{m-t-2,t\}}}$ values of c' mod p^κ (or likewise values of n mod p^κ) that yield solutions.

Note that c' ranges from 1 to $\frac{\phi(p^m)}{dp^t} = p^\kappa \frac{p^{m-\kappa-t-1}(p-1)}{d}$, giving

$$\frac{\phi(p^\kappa)}{dp^{\min\{m-t-2,t\}}}\left(\frac{p^{m-\kappa-t-1}(p-1)}{d}\right) = \frac{\phi^2(p)}{d^2}p^{\max\{m-2t-2,0\}}$$

c's that will allow a solution to our characteristic equation, and (5.9) is clear.

Similarly n ranges over the terms relatively prime to p from 1 to $p^m = p^\kappa(p^{m-\kappa})$,

$$\frac{\phi(p^\kappa)}{dp^{\min\{m-t-2,t\}}}p^{m-\kappa} = \frac{\phi(p)}{d}p^{\max\{m-t-1,t+1\}},$$

giving (5.10).

□

5.4 When $p = 2$, $m \geq 6$

We now examine the case when $p = 2$ and $m \geq 6$, giving sums of the form

$$S_1(\chi, nx^{\gamma 2^t}, 2^m) = \sum_{x=1}^{2^m} \chi(x)e_{2^m}(nx^{\gamma 2^t})$$

where χ is a character mod 2^m, n and γ are odd, and $t \geq 0$. Since $x^{2^{m-2}} \equiv 1 \bmod 2^m$ for any odd x we shall assume that

$$t < m - 2.$$

When dealing with these sums the methods are nearly the same except that we need two

generators, $a = 5$ and -1, to generate all of $\mathbb{Z}_{2^m}^*$. Even so, this case is actually simpler computation-wise. As for odd p we can also immediately say that $S_2(\chi, nx^k, 2^m) = 0$ unless $\chi = \chi_1^k$ for some character $\chi_1 \bmod 2^m$. The proof of this is almost the same the proof of Lemma 2.1 (we get the same relation for $\chi(a)$ and, when $m > 2$ and the second generator -1 is needed, taking $z = -1$ in the same argument gives $\chi(-1) = 1$ if k is even).

Here we write

$$\chi(a) = e\left(\frac{c}{2^{m-2}}\right)$$

and define the odd integer $R_{\lceil \frac{m}{2} \rceil}$ and when $t \geq 1$ the odd integer R_{t+2} by

$$a^{2^{\lceil \frac{m}{2} \rceil - 2}} = 1 + R_{\lceil \frac{m}{2} \rceil} 2^{\lceil \frac{m}{2} \rceil}, \quad a^{2^t} = 1 + R_{t+2} 2^{t+2}. \tag{5.30}$$

We will have $S_2(\chi, nx^{2^t\gamma}, 2^m) = 0$ unless $c = 2^t c'$ with c' odd, and our characteristic equation will take the form

$$c' + nR_{\lceil \frac{m}{2} \rceil} \gamma x^{2^t\gamma} \equiv 0 \bmod 2^{\lfloor \frac{m}{2} \rfloor}. \tag{5.31}$$

We first evaluate the sums

$$S(n) := \sum_{k=1}^{2^{m-2}} \chi(a^k) e_{2^m}(na^{k\gamma 2^t}).$$

Lemma 5.4.1. *Suppose that $c = 2^t c'$ with c' odd. If $0 \leq t < \lceil \frac{m}{2} \rceil - 2$ and (5.31) has a solution $\alpha = a^{v_0}$ then*

$$S(n) = 2^{\lfloor \frac{m}{2} \rfloor + t} \chi(\alpha) e_{2^m}(n\alpha^{\gamma 2^t}) \psi,$$

where

$$\psi = \begin{cases} 1, & \text{if } m \text{ is even,} \\ 1 + (-1)^{(\frac{\gamma-1}{2} + \lambda)} i^{R_{\lceil \frac{m}{2} \rceil} c'}, & \text{if } m \text{ is odd,} \end{cases} \tag{5.32}$$

with λ defined by

$$c' + nR_{\lceil \frac{m}{2} \rceil} \gamma \alpha^{\gamma 2^t} = \lambda 2^{\lfloor \frac{m}{2} \rfloor}. \tag{5.33}$$

If $\lceil \frac{m}{2} \rceil - 2 \leq t < m-2$ *and* $c' + nR_{t+2}\gamma \equiv 0 \ mod\ 2^{m-2-t}$ *then*

$$S(n) = 2^{m-2} e\left(\frac{n}{2^m}\right).$$

Otherwise $S(n) = 0$.

Proof.

$$S(n) = \sum_{k=1}^{2^{m-2}} e\left(\frac{kc}{2^{m-2}}\right) e_{2^m}(na^{k\gamma 2^t}).$$

If $t+2 \geq \lceil \frac{m}{2} \rceil$ then

$$na^{k\gamma 2^t} = n\left(1 + R_{t+2}2^{t+2}\right)^{k\gamma} \equiv n\left(1 + R_{t+2}k\gamma 2^{t+2}\right) \mod 2^m,$$

and

$$S(n) = e\left(\frac{n}{2^m}\right) \sum_{k=1}^{2^{m-2}} e\left(\frac{k(c + nR_{t+2}\gamma 2^t)}{2^{m-2}}\right).$$

The sum is 2^{m-2} if $c + nR_{t+2}\gamma 2^t \equiv 0 \mod 2^{m-2}$ (and zero otherwise). This only occurs when $c = 2^t c'$, c' odd, with $c' + nR_{t+2}\gamma \equiv 0 \mod 2^{m-t-2}$.

Suppose now that $t < \lceil \frac{m}{2} \rceil - 2$. We write $k = u2^{\lceil \frac{m}{2} \rceil - t - 2} + v$ where v runs through an interval I of length $2^{\lceil \frac{m}{2} \rceil - t - 2}$ and $u = 1, ..., 2^{\lfloor \frac{m}{2} \rfloor + t}$. Using (5.30) and expanding binomially gives

$$\begin{aligned} S(n) &= \sum_{v \in I} \sum_{u=1}^{2^{\lfloor \frac{m}{2} \rfloor + t}} e\left(\frac{(u2^{\lceil \frac{m}{2} \rceil - t - 2} + v)c}{2^{m-2}}\right) e\left(\frac{na^{(u2^{\lceil \frac{m}{2} \rceil - t - 2} + v)\gamma 2^t}}{2^m}\right) \\ &= \sum_{v \in I} \chi(a^v) e\left(\frac{na^{v\gamma 2^t}}{2^m}\right) \sum_{u=1}^{2^{\lfloor \frac{m}{2} \rfloor + t}} e\left(\frac{cu}{2^{\lfloor \frac{m}{2} \rfloor + t}}\right) e\left(\frac{na^{v\gamma 2^t}\left((1 + R_{\lceil \frac{m}{2} \rceil}2^{\lceil \frac{m}{2} \rceil})^{u\gamma} - 1\right)}{2^m}\right) \\ &= \sum_{v \in I} \chi(a^v) e\left(\frac{na^{v\gamma 2^t}}{2^m}\right) \sum_{u=1}^{2^{\lfloor \frac{m}{2} \rfloor + t}} e\left(\frac{u\left(c + nR_{\lceil \frac{m}{2} \rceil}\gamma 2^t a^{v\gamma 2^t}\right)}{2^{\lfloor \frac{m}{2} \rfloor + t}}\right). \end{aligned}$$

So as in our previous cases we end up with a sum over a full set of residues and the inner

sum is zero unless

$$c + nR_{\lceil \frac{m}{2} \rceil} \gamma 2^t a^{v\gamma 2^t} \equiv 0 \bmod 2^{\lfloor \frac{m}{2} \rfloor + t}.$$

In order to have a solution plainly $c = 2^t c'$ for some odd c', reducing our congruence to

$$c' + nR_{\lceil \frac{m}{2} \rceil} \gamma a^{v\gamma 2^t} \equiv 0 \bmod 2^{\lfloor \frac{m}{2} \rfloor}.$$

Thus $S(n) = 0$ unless we have a solution $\alpha = a^{v_0}$ to our characteristic equation (5.31). We take I to be the interval $\left[v_0, v_0 + 2^{\lceil \frac{m}{2} \rceil - t - 2}\right]$. If a^v is another solution then plainly

$$v\gamma 2^t \equiv v_0 \gamma 2^t \bmod 2^{\lfloor \frac{m}{2} \rfloor - 2},$$

and

$$v \equiv v_0 \bmod 2^{\lfloor \frac{m}{2} \rfloor - t - 2}.$$

When m is even $\lfloor \frac{m}{2} \rfloor = \lceil \frac{m}{2} \rceil$ and we only have the solution v_0 in our range for v, and

$$S(n) = 2^{\frac{m}{2} + t} \chi(\alpha) e_{2^m}(n\alpha^{\gamma 2^t}).$$

When m is odd we note that $2^{\lfloor \frac{m}{2} \rfloor - t - 2}$ is half the range of v and we have two solutions $\alpha = a^{v_0}$ and $a^{v_0 + 2^{\lfloor \frac{m}{2} \rfloor - t - 2}}$. Plugging these in, using that $a^{2^{\lfloor \frac{m}{2} \rfloor - 2}} = 1 + R_{\lfloor \frac{m}{2} \rfloor} 2^{\lfloor \frac{m}{2} \rfloor}$ for some odd $R_{\lfloor \frac{m}{2} \rfloor}$ when $m \geq 6$, and expanding binomially, we get

$$\begin{aligned}
S(n) &= 2^{\lfloor \frac{m}{2} \rfloor + t} \left(\chi(a^{v_0}) e_{2^m}(n(a^{v_0})^{\gamma 2^t}) + \chi(a^{v_0 + 2^{\lfloor \frac{m}{2} \rfloor - t - 2}}) e_{2^m}(n(a^{v_0 + 2^{\lfloor \frac{m}{2} \rfloor - t - 2}})^{\gamma 2^t} \right) \\
&= 2^{\lfloor \frac{m}{2} \rfloor + t} \chi(\alpha) e_{2^m}(n\alpha^{\gamma 2^t}) \left(1 + \chi(a^{2^{\lfloor \frac{m}{2} \rfloor - t - 2}}) e_{2^m}(n a^{v_0 \gamma 2^t} \left((1 + R_{\lfloor \frac{m}{2} \rfloor} 2^{\lfloor \frac{m}{2} \rfloor})^{\gamma} - 1 \right) \right) \\
&= 2^{\lfloor \frac{m}{2} \rfloor + t} \chi(\alpha) e_{2^m}(n\alpha^{\gamma 2^t}) \left(1 + e\left(\frac{c'}{2^{\lceil \frac{m}{2} \rceil}} \right) e\left(\frac{nR_{\lfloor \frac{m}{2} \rfloor} \gamma 2^{\lfloor \frac{m}{2} \rfloor} a^{v_0 2^t \gamma} + \frac{\gamma(\gamma-1)}{2} n (R_{\lfloor \frac{m}{2} \rfloor})^2 2^{m-1} a^{v_0 \gamma 2^t}}{2^m} \right) \right) \\
&= 2^{\lfloor \frac{m}{2} \rfloor + t} \chi(\alpha) e_{2^m}(n\alpha^{\gamma 2^t}) \left(1 + (-1)^{\frac{\gamma - 1}{2}} e\left(\frac{c' + nR_{\lfloor \frac{m}{2} \rfloor} \gamma a^{v_0 \gamma 2^t}}{2^{\lceil \frac{m}{2} \rceil}} \right) \right).
\end{aligned}$$

We note that $a^{2^{\lceil \frac{m}{2} \rceil - 2}} = 1 + R_{\lceil \frac{m}{2} \rceil} 2^{\lceil \frac{m}{2} \rceil} = (1 + R_{\lfloor \frac{m}{2} \rfloor} 2^{\lfloor \frac{m}{2} \rfloor})^2 = (a^{2^{\lfloor \frac{m}{2} \rfloor - 2}})^2$ giving us that

$$R_{\lfloor \frac{m}{2} \rfloor} = R_{\lceil \frac{m}{2} \rceil} - (R_{\lfloor \frac{m}{2} \rfloor})^2 2^{\lfloor \frac{m}{2} \rfloor - 1} \equiv R_{\lceil \frac{m}{2} \rceil} - 2^{\lfloor \frac{m}{2} \rfloor - 1} \bmod 2^{\lceil \frac{m}{2} \rceil}.$$

Plugging this in for $R_{\lfloor \frac{m}{2} \rfloor}$ we get

$$\begin{aligned} e\left(\frac{c' + nR_{\lfloor \frac{m}{2} \rfloor} \gamma a^{v_0 \gamma 2^t}}{2^{\lceil \frac{m}{2} \rceil}}\right) &= e\left(\frac{c' + nR_{\lceil \frac{m}{2} \rceil} \gamma a^{v_0 \gamma 2^t}}{2^{\lceil \frac{m}{2} \rceil}}\right) e\left(\frac{-n\gamma a^{v_0 \gamma 2^t}}{2^2}\right) \\ &= e\left(\frac{\lambda}{2}\right) e\left(\frac{c' R_{\lceil \frac{m}{2} \rceil}}{4}\right), \end{aligned}$$

(using the characteristic equation and that $\left\lfloor \frac{m}{2} \right\rfloor \geq 2$) and the claimed result follows.

□

Theorem 5.4.1. *Suppose that χ is a 2^tth power of a primitive character mod 2^m. If $0 \leq t < \left\lceil \frac{m}{2} \right\rceil - 2$ and (5.31) has a solution α then, with ψ as in (5.32),*

$$S_1(\chi, nx^{\gamma 2^t}, 2^m) = 2^{\lfloor \frac{m}{2} \rfloor + t + \delta} \chi(\alpha) e_{2^m}(n\alpha^{\gamma 2^t}) \psi, \quad \delta = \begin{cases} 0, & \text{if } t = 0, \\ 1, & \text{if } t > 0. \end{cases}$$

If $\left\lceil \frac{m}{2} \right\rceil - 2 \leq t < m - 2$ and $c' + nR_{t+2}\gamma \equiv 0 \bmod 2^{m-2-t}$ then

$$S_1(\chi, nx^{\gamma 2^t}, 2^m) = 2^{m-1} e\left(\frac{n}{2^m}\right).$$

Otherwise $S_1(\chi, nx^{\gamma 2^t}, 2^m) = 0$.

Thus for $m \geq 6$ the non-zero values satisfy

$$\left|S_1(\chi, nx^{\gamma 2^t}, 2^m)\right| = 2^\tau, \quad \tau = \begin{cases} \frac{m}{2}, & \text{if } t = 0, \\ \frac{m}{2} + t + 1, & \text{if } 0 < t < \left\lceil \frac{m}{2} \right\rceil - 2, \\ m - 1, & \text{if } \left\lceil \frac{m}{2} \right\rceil - 2 \leq t < m - 2. \end{cases} \tag{5.34}$$

Proof. We start by writing the sum in terms of the generators, -1 and a, of $\mathbb{Z}_{2^m}^*$,

$$\begin{aligned} S_1(\chi, nx^{\gamma 2^t}, 2^m) &= \sum_{x=1}^{2^m} \chi(x) e_{2^m}(nx^{\gamma 2^t}) \\ &= \sum_{\omega=0}^{1} \sum_{k=1}^{2^{m-2}} \chi((-1)^\omega a^k) e_{2^m}(n((-1)^\omega a^k)^{\gamma 2^t}) \\ &= S(n) + \chi(-1) S((-1)^{2^t} n). \end{aligned}$$

If $t = 0$ then

$$S_1(\chi, nx^{\gamma 2^t}, 2^m) = S(n) + \chi(-1) S(-n).$$

By the lemma each $S(\pm n)$ is zero unless (5.31) has a solution α. A solution will be either of the form $\alpha = a^{v_0}$ or $-a^{v_0}$ (since $m \geq 6$ we can not have solutions of both forms). By Lemma 5.4.1, in the first case $S(-n) = 0$ and

$$S_1(\chi, nx^{\gamma 2^t}, 2^m) = S(n) = 2^{\lfloor \frac{m}{2} \rfloor} \chi(\alpha) e_{2^m}(n\alpha^\gamma) \psi.$$

In the second case $S(n) = 0$ and

$$S_1(\chi, nx^{\gamma 2^t}, 2^m) = \chi(-1) S(-n) = \chi(-1) 2^{\lfloor \frac{m}{2} \rfloor} \chi(-\alpha) e_{2^m}(-n(-\alpha)^\gamma) \psi.$$

If $t > 0$

$$S_1(\chi, nx^{\gamma 2^t}, 2^m) = S(n) + \chi(-1) S(n)$$

Thus if $\chi(-1) = -1$ our sum is zero. Otherwise

$$S_1(\chi, nx^{\gamma^{2^t}}, 2^m) = 2S(n)$$

and the result follows from the lemma.

□

Chapter 6

Evaluating the Binomial Character Sums Modulo Prime Powers

In this section we show that the multiplicative character sums,

$$S^*(\chi, x^l(Ax^k + B)^w, p^m) = \sum_{\substack{x=1 \\ p \nmid x}}^{p^m} \chi(x^l(Ax^k + B)^w) \tag{6.1}$$

have a simple evaluation for large enough m. In particular, if $p \nmid ABk$, we can evaluate (6.1) for $m \geq 2$. Equivalently, for characters χ_1 and χ_2 mod p^m we define

$$S_2 = S(\chi_1, \chi_2, Ax^k + B, p^m) = \sum_{x=1}^{p^m} \chi_1(x)\chi_2(Ax^k + B). \tag{6.2}$$

These include the mod p^m generalizations of the classical Jacobi sums

$$J(\chi_1, \chi_2, p^m) = \sum_{x=1}^{p^m} \chi_1(x)\chi_2(1 - x). \tag{6.3}$$

We note that the classical Jacobi Sum is zero if $p = 2$. However, for the general case (6.2) the sum may be nonzero for $p = 2$, e.g. if A is off and B is even. In Chapter 7 we consider

multi variable Jacobi sums. See [2] or [14] for an extensive treatment of mod p Jacobi sums and their generalizations over $\mathbb{F}_{p^m}$.

These sums have been evaluated exactly by Zhang Wenpeng & Weili Yao [30] when χ_1, χ_2 and $\chi_1\chi_2$ are primitive and $m \geq 2$ is even (some generalizations are considered in [32]).

Writing

$$\chi_1 = \chi^l, \quad \chi_2 = \chi^w, \quad \chi_1(x)\chi_2(Ax^k + B) = \chi(x^l(Ax^k + B)^w), \tag{6.4}$$

with $\chi_1 = \chi_0$ the principal character if $l = 0$, the correspondence between (6.1) and (6.2) is clear. Of course the restriction $p \nmid x$ in (6.1) only differs from $\sum^*$ when $l = 0$. We shall assume throughout that χ_2 is a primitive character mod p^m (equivalently χ is primitive and $p \nmid w$); if χ_2 is not primitive but χ_1 is primitive then $S(\chi_1, \chi_2, Ax^k + B, p^m) = 0$ (since $\sum_{y=1}^{p} \chi_1(x + yp^{m-1}) = 0$), if both are not primitive we can reduce to a lower modulus $S(\chi_1, \chi_2, Ax^k + B, p^m) = pS(\chi_1, \chi_2, Ax^k + B, p^{m-1})$.

It is interesting that the sum (6.1) can be written explicitly in terms of classical Gauss sums for any $m \geq 1$. In particular one can trivially recover the Weil bound in these cases. We explore this in Section 2.

We assume, noting the correspondence (6.4) between (6.1) and (6.2), that

$$g(x) = x^l(Ax^k + B)^w, \quad p \nmid w \tag{6.5}$$

where k, l are integers with $k > 0$ (else $x \mapsto x^{-1}$) and A, B non-zero integers with

$$A = p^n A', \quad 0 \leq n < m, \quad p \nmid A'B. \tag{6.6}$$

We define the integers $d \geq 1$ and $t \geq 0$ by

$$d = (k, p - 1), \qquad p^t \mid\mid k. \tag{6.7}$$

For $m \geq n+t+1$ by Lemma 2.3.1 it transpires that the sum in (6.1) or (6.2) is zero unless

$$\chi_1 = \chi_3^k, \tag{6.8}$$

for some mod p^m character, χ_3 (i.e. χ is the $(k, \phi(p^m))/(k, l, \phi(p^m))$-th power of a character). This condition will also arise naturally in our proof. In order for the sum to be nonzero we must also have a solution, x_0, to a characteristic equation of the form,

$$g'(x) \equiv 0 \bmod p^{\min\left\{m-1, [\frac{m+n}{2}]+t\right\}} \tag{6.9}$$

with

$$p \nmid x_0(Ax_0^k + B). \tag{6.10}$$

Notice that in order to have a solution to (6.9) we must have

$$p^{n+t} \mid\mid l, \quad p^t \mid\mid l + wk, \tag{6.11}$$

if $m > t+n+1$ (equivalently χ_1 is induced by a primitive mod p^{m-n-t} character and $\chi_1\chi_2^w$ is a primitive mod p^{m-t} character) and $p^{n+t} \mid l$ if $m = t+n+1$.

When (6.8) holds, (6.9) has a solution x_0 satisfying (6.10) and $m > n+t+1$, Theorem 6.1.1 below gives an explicit evaluation of the sum (6.2). From this we see that for any odd prime p,

$$\left|\sum_{x=1}^{p^m} \chi_1(x)\chi_2(Ax^k+B)\right| = \begin{cases} dp^{m-1}, & \text{if } t+n+1 < m \leq 2t+n+2, \\ dp^{\frac{m+n}{2}+t}, & \text{if } 2t+n+2 < m. \end{cases} \tag{6.12}$$

The condition $m > t+n+1$ is natural here; if $t \geq m-n$ then one can of course use Euler's Theorem to reduce the power of p in k to $t = m-n-1$. If $t = m-n-1$ and the sum is non-zero then, as in a Heilbronn sum, we obtain a mod p sum, $p^{m-1}\sum_{x=1}^{p-1}\chi(x^l(Ax^k+B)^w)$,

where one does not expect a nice evaluation. For $t = 0$ the result (6.12) can be obtained from [6] by showing equality in their S_α evaluated at the d critical points α. For $t > 0$ the α will not have multiplicity one as needed in [6].

Finally, recalling Section 2.2, if χ is a mod rs character with $(r, s) = 1$, then $\chi = \chi_1\chi_2$ for a mod r character χ_1 and mod s character χ_2, and for any $g(x)$ in $\mathbb{Z}[x]$

$$\sum_{x=1}^{rs} \chi(g(x)) = \sum_{x=1}^{r} \chi_1(g(x)) \sum_{x=1}^{s} \chi_2(g(x)).$$

Thus it is enough to work modulo prime powers.

6.1 Evaluation of the Sums for p Odd

Theorem 6.1.1. *Suppose that p is an odd prime and χ_1, χ_2 are mod p^m characters with χ_2 primitive.*

If χ_1 satisfies (6.8), and (6.9) has a solution x_0 satisfying (6.10), then

$$\sum_{x=1}^{p^m} \chi_1(x)\chi_2(Ax^k + B) = d\chi(g(x_0)) \begin{cases} p^{m-1}, & \text{if } t + n + 1 < m \leq 2t + n + 2, \\ p^{\frac{m+n}{2}+t}, & \text{if } m > 2t + n + 2,\ m - n \text{ even}, \\ p^{\frac{m+n}{2}+t}\varepsilon_1, & \text{if } m > 2t + n + 2,\ m - n \text{ odd}, \end{cases}$$

where n, d, t and g are as defined in (6.6), (6.7) and (6.5), with

$$\varepsilon_1 = \left(\frac{\alpha}{p}\right) e_p\left(-2^{-2}\beta^2\alpha^{-1}\right) \varepsilon, \qquad \varepsilon = \begin{cases} 1 & p \equiv 1 \bmod 4, \\ i & p \equiv 3 \bmod 4, \end{cases} \tag{6.13}$$

where α and β are integers defined in (6.21) below and $\left(\frac{\alpha}{p}\right)$ is the Legendre symbol.

If χ_1 does not satisfy (6.8), or (6.9) has no solution satisfying (6.10), then the sum is

zero.

Note $e_p\left(-2^{-2}\beta^2\alpha^{-1}\right) = 1$ if the solution to (6.9) satisfies the stronger congruence, mod $p^{\left[\frac{m+n}{2}\right]+t+1}$.

For the mod p^m Jacobi sums, $\chi_1 = \chi^l$, $\chi_2 = \chi^w$, χ primitive mod p^m with $p \nmid lw(l+w)$, we have $x_0 = l(l+w)^{-1}$ and

$$\sum_{x=1}^{p^m} \chi_1(x)\chi_2(1-x) = \frac{\chi_1(l)\chi_2(w)}{\chi_1\chi_2(l+w)} p^{\frac{m}{2}} \begin{cases} 1, & \text{if } m \text{ is even,} \\ \left(\frac{-2rc}{p}\right)\left(\frac{lw(l+w)}{p}\right)\varepsilon, & \text{if } m \geq 3 \text{ is odd,} \end{cases}$$

with r and c as in (2.8) and (2.10).

Proof. Recall that a is a primitive root for all powers of p and we define the integers R_l, $p \nmid R_l$, by

$$a^{\phi(p^l)} = 1 + R_l p^l,$$

so that $r = R_1$. Since $(1 + R_{s+1}p^{s+1}) = (1 + R_s p^s)^p$, for any $s \geq 1$ we recall

$$R_{s+1} \equiv R_s \bmod p^s. \tag{6.14}$$

We define the integers c, $c_1 = cl$, $c_2 = cw$, by

$$\chi(a) = e_{\phi(p^m)}(c), \quad \chi_1(a) = e_{\phi(p^m)}(c_1), \quad \chi_2(a) = e_{\phi(p^m)}(c_2). \tag{6.15}$$

Since χ_2 is assumed primitive we have $p \nmid c_2$.

We write

$$\gamma = u\frac{\phi(p^L)}{d} + v, \qquad L := \begin{cases} 1, & \text{if } m \leq n + 2t + 2, \\ \left\lceil \frac{m-n}{2} \right\rceil - t, & \text{if } m > n + 2t + 2, \end{cases}$$

and observe that if $u = 1, ..., dp^{m-L}$ and v runs through an interval I of length $\phi(p^L)/d$ then γ runs through a complete set of residues mod $\phi(p^m)$. Hence setting $h(x) = Ax^k + B$ and writing $x = a^\gamma$ we have

$$\sum_{x=1}^{p^m} \chi_1(x)\chi_2(h(x)) = \sum_{v\in I} \chi_1(a^v) \sum_{u=1}^{dp^{m-1}} \chi_1(a^{u\frac{\phi(p^L)}{d}})\chi_2\left(h\left(a^{u\frac{\phi(p^L)}{d}+v}\right)\right).$$

Since $2(L+t)+n \geq m$ we can write

$$\begin{aligned} h\left(a^{u\frac{\phi(p^L)}{d}+v}\right) &= A\left(a^{\phi(p^{L+t})}\right)^{u\left(\frac{k}{dp^t}\right)} a^{vk} + B = A\left(1+R_{L+t}p^{L+t}\right)^{u\left(\frac{k}{dp^t}\right)} a^{vk} + B \\ &\equiv h(a^v) + A'u\left(\frac{k}{dp^t}\right) a^{vk} R_{L+t} p^{L+t+n} \bmod p^m. \end{aligned}$$

This is zero mod p if $p \mid h(a^v)$ and consequently any such v give no contribution to the sum. If $p \nmid h(a^v)$ then, since $R_{L+t} \equiv R_{L+t+n} \bmod p^{L+t}$,

$$\begin{aligned} h\left(a^{u\frac{\phi(p^L)}{d}+v}\right) &\equiv h(a^v)\left(1 + A'u\left(\frac{k}{dp^t}\right) h(a^v)^{-1} a^{vk} R_{L+t+n} p^{L+t+n}\right) \bmod p^m \\ &\equiv h(a^v) a^{A'u\left(\frac{k}{dp^t}\right) h(a^v)^{-1} a^{vk} \phi(p^{L+t+n})} \bmod p^m. \end{aligned}$$

Thus,

$$\sum_{x=1}^{p^m} \chi_1(x)\chi_2(h(x)) = \sum_{\substack{v\in I \\ p\nmid h(a^v)}} \chi_1(a^v)\chi_2(h(a^v)) \sum_{u=1}^{dp^{m-L}} \chi_1\left(a^{u\frac{\phi(p^L)}{d}}\right) \chi_2\left(a^{u\frac{\phi(p^L)}{d} Aka^{vk} h(a^v)^{-1}}\right),$$

where the inner sum $\sum_{u=1}^{dp^{m-L}} e_{dp^{m-L}}\left(u\left(c_1 + c_2 A h(a^v)^{-1} k a^{vk}\right)\right)$ is dp^{m-L} if

$$c_1 + c_2 h(a^v)^{-1} A' a^{vk} \left(\frac{k}{dp^t}\right) dp^{t+n} \equiv 0 \bmod dp^{m-L} \tag{6.16}$$

and zero otherwise. Thus our sum will be zero unless (6.16) has a solution with $p \nmid h(a^v)$. For $m \geq n+t+1$ we have $m - L \geq t + n$ and a solution to (6.16) necessitates $dp^{t+n} \mid c_1$ (giving us condition (6.8)) with $p^{t+n} \mid\mid l$ for $m > n+t+1$. Hence for $m > n+t+1$ we can simplify the congruence to

$$h(a^v)\left(\frac{c_1}{dp^{t+n}}\right) + c_2 A' a^{vk}\left(\frac{k}{dp^t}\right) \equiv 0 \bmod p^{m-L-t-n}, \tag{6.17}$$

and for a solution we must have $p^t \mid\mid c_1 + kc_2$. Equivalently,

$$\frac{cg'(a^v)}{dp^{t+n}} \equiv 0 \bmod p^{m-t-n-L}, \tag{6.18}$$

and the characteristic equation (6.9) must have a solution satisfying (6.10). Suppose that (6.9) has a solution $x_0 = a^{v_0}$ with $p \nmid h(x_0)$ and that $m > n+t+1$. Rewriting the congruence (6.18) in terms of the primitive root, a, gives

$$a^{vk} \equiv a^b \bmod p^{m-t-n-L}$$

for some integer b. Thus two solutions to (6.18), a^{v_1} and a^{v_2} must satisfy

$$v_1 k \equiv v_2 k \bmod \phi(p^{m-t-n-L}).$$

That is $v_1 \equiv v_2 \bmod \frac{(p-1)}{d}$ if $m \leq n + 2t + 2$ and if $m > n + 2t + 2$

$$v_1 \equiv v_2 \bmod \frac{\phi(p^{m-n-2t-L})}{d}$$

where $m-n-2t-L=L$ if $m-n$ is even and $L-1$ if $m-n$ is odd. Thus if $n+t+1<m\le n+2t+2$ or $m>n+2t+2$ and $m-n$ is even our interval I contains exactly one solution v. Choosing I to contain v_0 we get that

$$\sum_{x=1}^{p^m}\chi_1(x)\chi_2(h(x))=dp^{m-L}\chi_1(x_0)\chi_2(h(x_0)).$$

Suppose that $m>n+2t+2$ with $m-n$ odd and set $s:=\frac{m-n-1}{2}$. In this case I will have p solutions and we pick our interval I to contain the p solutions $v_0+yp^{s-t-1}\left(\frac{p-1}{d}\right)$ where $y=0,...,p-1$. Since $dp^t\mid c_1$ and $dp^t\mid k$ we can write, with g defined as in (6.5),

$$g_1(x):=g(x)^c=x^{c_1}(Ax^k+B)^{c_2}=:H\left(x^{dp^t}\right).$$

Thus, setting $\chi=\chi_4^c$, where χ_4 is the mod p^m character with $\chi_4(a)=e_{\phi(p^m)}(1)$,

$$\begin{aligned}\sum_{x=1}^{p^m}\chi_1(x)\chi_2(h(x))&=dp^{\frac{m+n-1}{2}+t}\sum_{y=0}^{p-1}\chi\left(g\left(a^{v_0+yp^{s-t-1}\left(\frac{p-1}{d}\right)}\right)\right)\\&=dp^{\frac{m+n-1}{2}+t}\sum_{y=0}^{p-1}\chi_4\left(H\left(x_0^{dp^t}a^{y\phi(p^s)}\right)\right),\end{aligned}$$

where

$$x_0^{dp^t}a^{y\phi(p^s)}=x_0^{dp^t}\left(1+R_sp^s\right)^y=x_0^{dp^t}+yR_sx_0^{dp^t}p^s \bmod p^{m-n-1}. \tag{6.19}$$

Since

$$p^{-n}H'(x^{dp^t})=\left(\frac{xg_1'(x)}{dp^{t+n}}\right)x^{-dp^t}\in\mathbb{Z}[x],$$

we have $p^n\mid\frac{H^{(k)}\left(x_0^{dp^t}\right)}{k!}$, for all $k\ge1$. As $xg_1'(x)=(c_1+kc_2)g_1(x)-c_2kBg_1(x)/h(x)$,

$$p^{-n}H''(x^{dp^t})x^{2dp^t}=\left(\frac{c_1}{dp^t}+c_2\frac{k}{dp^t}-c_2\frac{k}{dp^t}\frac{B}{h(x)}-1\right)\left(\frac{xg_1'(x)}{dp^{t+n}}\right)+c_2\left(\frac{k}{dp^t}\right)^2A'Bx^k\frac{g_1(x)}{h(x)^2}.$$

Plainly a solution x_0 to (6.9) satisfying (6.10) also has $g_1'(x_0) \equiv 0 \bmod p^{\frac{m+n-1}{2}+t}$ and

$$\frac{x_0 g_1'(x_0)}{dp^{t+n}} = \lambda p^{\frac{m-n-1}{2}}, \qquad H'(x_0^{dp^t}) = x_0^{-dp^t} \lambda p^{\frac{m+n-1}{2}}, \tag{6.20}$$

for some integer λ, and

$$p^{-n} H''(x_0^{dp^t}) \equiv c_2 \left(\frac{k}{dp^t}\right)^2 A' B x_0^{k-2dp^t} \frac{g_1(x_0)}{h(x_0)^2} \bmod p.$$

Hence by the Taylor expansion, using (6.19) and that $R_s \equiv R_{m-1} \equiv r \bmod p$,

$$\begin{aligned} H\left(x_0^{dp^t} a^{y\phi(p^s)}\right) &\equiv H(x_0^{dp^t}) + H'(x_0^{dp^t}) y R_s x_0^{dp^t} p^{\frac{m-n-1}{2}} + 2^{-1} H''(x_0^{dp^t}) y^2 R_s^2 x_0^{2dp^t} p^{m-n-1} \bmod p^m \\ &\equiv g_1(x_0)\left(1 + \left(\beta y + \alpha y^2\right) R_{m-1} p^{m-1}\right) \bmod p^m \\ &\equiv g_1(x_0) a^{\left(\beta y + \alpha y^2\right)\phi(p^{m-1})} \bmod p^m, \end{aligned}$$

with

$$\beta := g_1(x_0)^{-1}\lambda, \qquad \alpha := 2^{-1} c_2 h(x_0)^{-2} r A' B \left(\frac{k}{dp^t}\right)^2 x_0^k, \tag{6.21}$$

and

$$\chi_4\left(H\left(x_0^{dp^t} a^{y\phi(p^s)}\right)\right) = \chi(g(x_0)) e_p(\alpha y^2 + \beta y).$$

Since plainly $p \nmid \alpha$, completing the square then gives the result claimed

$$\begin{aligned} \sum_{x=1}^{p^m} \chi_1(x)\chi_2(h(x)) &= dp^{\frac{m+n-1}{2}+t} \chi(g(x_0)) e_p(-4^{-1}\alpha^{-1}\beta^2) \sum_{y=0}^{p} e_p(\alpha y^2) \\ &= dp^{\frac{m+n-1}{2}+t} \chi(g(x_0)) e_p(-4^{-1}\alpha^{-1}\beta^2) \left(\frac{\alpha}{p}\right) \varepsilon p^{\frac{1}{2}} \end{aligned}$$

where ε is 1 or i as p is 1 or 3 mod 4. Notice that if x_0 is a solution to the stronger congruence $g'(x_0) \equiv 0 \bmod p^{\left[\frac{m+n}{2}\right]+t+1}$ then $\beta = 0$ and the $e_p(-4^{-1}\alpha^{-1}\beta^2)$ can be omitted. □

6.2 Evaluating the Binomial Character Sum for $p = 2$

Suppose that χ_1 and χ_2 are mod 2^m multiplicative characters with χ_2 primitive mod 2^m, $m \geq 3$. This section represents joint work with Chris Pinner and Joe Sheppard [22] in which we evaluate the complete character sum

$$S_2 := \sum_{x=1}^{2^m} \chi_1(x)\chi_2(Ax^k + B). \tag{6.22}$$

Plainly $S_2 = 0$ if A and B are not of opposite parity (otherwise x or $Ax^k + B$ will be even and the individual terms will all be zero). We assume here that A is even and B is odd and write

$$A = 2^n A_1,\ n > 0, \quad k = 2^t k_1, \quad 2 \nmid A_1 k_1 B.$$

If B is even and A odd we can use $x \mapsto x^{-1}$ to write S_2 in the form

$$S_2 = \sum_{x=1}^{2^m} \overline{\chi_1 \chi_2^k}(x)\chi_2(Bx^k + A).$$

Since $\mathbb{Z}_{2^m}^* =< -1, 5 >$, the characters χ_1, χ_2 are completely determined by their values on -1 and 5. Since 5 has order 2^{m-2} mod 2^m we can define integers c_1, c_2 with

$$\chi_i(5) = e_{2^{m-2}}(c_i), \quad 1 \leq c_i \leq 2^{m-2},$$

where $e_n(x) := e^{2\pi i x/n}$. Since χ_2 is primitive we have $2 \nmid c_2$. We define the odd integers R_i, $i \geq 2$, by

$$5^{2^{i-2}} = 1 + R_i 2^i. \tag{6.23}$$

Defining

$$N := \begin{cases} \lceil \frac{1}{2}(m-n) \rceil, & \text{if } m - n > 2t + 4, \\ t + 2, & \text{if } t + 2 \leq m - n \leq 2t + 4, \end{cases}$$

and

$$C(x) := c_1(Ax^k + B) + c_2 Akx^k R_N R_{N+n}^{-1} \tag{6.24}$$

(here and throughout this section y^{-1} denotes the inverse of y mod 2^m) it transpires that the sum S_2 will be zero unless there is a solution x_0 to the characteristic equation

$$C(x_0) \equiv 0 \bmod 2^{\lfloor \frac{1}{2}(m+n) \rfloor + t}, \tag{6.25}$$

with $2 \nmid x_0(Ax_0^k + B)$, when $m - n > 2t + 4$, and a solution to $C(1)$ or $C(-1) \equiv 0 \bmod 2^{m-2}$ when $t + 2 \leq m - n \leq 2t + 4$.

Theorem 6.2.1. *Suppose that $m - n \geq t + 2$. The sum $S_2 = 0$ unless $c_1 = 2^{n+t}c_3$, with $2 \nmid c_3$, and $\chi_1(-1) = 1$ when k is even, and the characteristic equation (6.25) has an odd solution x_0 when $m - n > 2t + 4$. Assume these conditions do hold.*

When $m - n > 2t + 4$,

$$S_2 = 2^{\frac{1}{2}(m+n)+t+\min\{1,t\}} \chi_1(x_0)\chi_2(Ax_0^k + B) \begin{cases} 1, & \text{if } m-n \text{ is even,} \\ \omega^h \left(\frac{2}{h}\right), & \text{if } m-n \text{ is odd,} \end{cases}$$

where $\left(\frac{2}{x}\right)$ is the Jacobi symbol, $\omega = e^{\pi i/4}$, $C(x_0) = \lambda 2^{\lfloor \frac{1}{2}(m+n) \rfloor + t}$ for some integer λ and $h := 2\lambda + (k_1 - 1) + (2^n - 1)c_3$.

When $t + 3 < m - n \leq 2t + 4$,

$$S_2 = \begin{cases} 2^{m-1}\chi_2(A + B), & \text{if } k \text{ is even and } C(1) \equiv 0 \bmod 2^{m-2}, \\ 2^{m-2}\chi_2(A + B), & \text{if } k \text{ is odd and } C(1) \equiv 0 \bmod 2^{m-2}, \\ 2^{m-2}\chi_1(-1)\chi_2(-A + B), & \text{if } k \text{ is odd and } C(-1) \equiv 0 \bmod 2^{m-2}, \\ 0, & \text{otherwise.} \end{cases}$$

When $m-n=t+3$,

$$S_2=\begin{cases}2^{m-1}\chi_2(A+B), & \text{if } k \text{ is even and } \chi_1(5)=\pm 1,\ \chi_1(-1)=1,\\ 2^{m-2}\left(\chi_2(A+B)+\chi_1(-1)\chi_2(-A+B)\right), & \text{if } k \text{ is odd and } \chi_1(5)=\pm 1,\\ 0, & \text{otherwise.}\end{cases}$$

When $m-n=t+2$,

$$S_2=\begin{cases}2^{m-1}\chi_2(A+B), & \text{if } k \text{ is even and } \chi_1=\chi_0 \text{ or } k \text{ is odd and } \chi_1=\chi_4,\\ 0, & \text{otherwise,}\end{cases}$$

where χ_0 *is the principal character mod* 2^m *and* χ_4 *is the mod* 2^m *character induced by the non-trivial character mod* 4 *(i.e.* $\chi_4(x)=\pm 1$ *as* $x\equiv\pm 1$ *mod* 4 *respectively).*

Note that the restriction $m-n\geq t+2$ is quite natural; for $m-n<t+2$ the odd x have $Ax^k+B\equiv A+B \bmod 2^m$ and $S_2=\chi_2(A+B)\sum_{x=1}^{2^m}\chi_1(x)=2^{m-1}\chi_2(A+B)$ if $\chi_1=\chi_0$ and zero otherwise.

Our original assumption that χ_2 is primitive is also reasonable; if χ_1 and χ_2 are both imprimitive then one should reduce the modulus, while if χ_1 is primitive and χ_2 imprimitive then $S_2=0$ (if χ_1 is primitive then $u=1+2^{m-1}$ must have $\chi_1(u)=-1$, since $x+2^{m-1}\equiv ux \bmod 2^m$ for any odd x, and $x\mapsto xu$ gives $S_2=\chi_1(u)S_2$ when χ_2 is imprimitive).

6.3 Proof of Theorem 6.2.1

6.3.1 Initial decomposition

Observing that $\pm 5^\gamma$, $\gamma = 1, \dots, 2^{m-2}$, gives a reduced residue system mod 2^m and writing

$$S(A) := \sum_{\gamma=1}^{2^{m-2}} \chi_1(5^\gamma)\chi_2(A5^{\gamma k} + B),$$

if k is even we have

$$S_2 = (1 + \chi_1(-1))S(A) = \begin{cases} 0, & \text{if } \chi_1(-1) = -1, \\ 2S(A), & \text{if } \chi_1(-1) = 1, \end{cases} \tag{6.26}$$

and if k is odd

$$S_2 = S(A) + \chi_1(-1)S(-A). \tag{6.27}$$

6.3.2 Large m values: $m > n + 2t + 4$

If I_1 is an interval of length $2^{\lceil \frac{m-n}{2} \rceil - t - 2}$ then plainly

$$\gamma = u2^{\lceil \frac{m-n}{2} \rceil - t - 2} + v, \quad v \in I_1, \quad u \in I_2 := \left[1, 2^{\lfloor \frac{m+n}{2} \rfloor + t}\right],$$

runs through a complete set of residues mod 2^{m-2}. Hence, writing $h(x) := Ax^k + B$ and noting that $2 \nmid h(5^v)$,

$$\begin{aligned} S(A) &= \sum_{v \in I_1} \chi_1(5^v) \sum_{u \in I_2} \chi_1\left(5^{u2^{\lceil \frac{m-n}{2} \rceil - t - 2}}\right) \chi_2\left(A5^{vk}5^{ku2^{\lceil \frac{m-n}{2} \rceil - t - 2}} + B\right) \\ &= \sum_{v \in I_1} \chi_1(5^v)\chi_2(h(5^v)) \sum_{u \in I_2} \chi_1\left(5^{u2^{\lceil \frac{m-n}{2} \rceil - t - 2}}\right) \chi_2(W) \end{aligned}$$

where

$$W = h(5^v)^{-1} A 5^{vk} \left(5^{ku2^{\lceil \frac{m-n}{2} \rceil - t - 2}} - 1 \right) + 1.$$

Since $n + 2\lceil \frac{m-n}{2} \rceil \geq m$ and $2\lceil \frac{m+n}{2} \rceil \geq m$ we have

$$\begin{aligned}
W &= A_1 5^{vk} h(5^v)^{-1} 2^n \left(\left(1 + R_{\lceil \frac{m-n}{2} \rceil} 2^{\lceil \frac{m-n}{2} \rceil} \right)^{uk_1} - 1 \right) + 1 \\
&\equiv 1 + A_1 5^{vk} h(5^v)^{-1} u k_1 R_{\lceil \frac{m-n}{2} \rceil} 2^{\lceil \frac{m+n}{2} \rceil} \bmod 2^m \\
&\equiv \left(1 + R_{\lceil \frac{m+n}{2} \rceil} 2^{\lceil \frac{m+n}{2} \rceil} \right)^{A_1 5^{vk} h(5^v)^{-1} u k_1 R_{\lceil \frac{m-n}{2} \rceil} R^{-1}_{\lceil \frac{m+n}{2} \rceil}} \bmod 2^m \\
&= 5^{A_1 5^{vk} h(5^v)^{-1} u k_1 R_{\lceil \frac{m-n}{2} \rceil} R^{-1}_{\lceil \frac{m+n}{2} \rceil} 2^{\lceil \frac{m+n}{2} \rceil - 2}} \\
&= 5^{A 5^{vk} h(5^v)^{-1} u k R_{\lceil \frac{m-n}{2} \rceil} R^{-1}_{\lceil \frac{m+n}{2} \rceil} 2^{\lceil \frac{m-n}{2} \rceil - t - 2}}.
\end{aligned}$$

We can write

$$\sum_{u \in I_2} \chi_1 \left(5^{u2^{\lceil \frac{m-n}{2} \rceil - t - 2}} \right) \chi_2(W) = \sum_{u \in I_2} e_{2^{\lfloor \frac{m+n}{2} \rfloor + t}} \left(u \left(c_1 + c_2 A 5^{vk} h(5^v)^{-1} k R_{\lceil \frac{m-n}{2} \rceil} R^{-1}_{\lceil \frac{m+n}{2} \rceil} \right) \right),$$

which equals $2^{\lfloor \frac{m+n}{2} \rfloor + t}$ for the v with

$$c_1 h(5^v) + c_2 A 5^{vk} k R_{\lceil \frac{m-n}{2} \rceil} R^{-1}_{\lceil \frac{m+n}{2} \rceil} \equiv 0 \bmod 2^{\lfloor \frac{m+n}{2} \rfloor + t} \tag{6.28}$$

and zero otherwise. Since $m \geq n + 2$ equation (6.28) has no solution (and hence $S_2 = 0$) unless $c_1 = 2^{n+t} c_3$ with $2 \nmid c_3$, in which case (6.28) becomes

$$\left(c_3 A + c_2 A_1 k_1 R_{\lceil \frac{m-n}{2} \rceil} R^{-1}_{\lceil \frac{m+n}{2} \rceil} \right) 5^{vk} \equiv -c_3 B \bmod 2^{\lfloor \frac{m-n}{2} \rfloor}. \tag{6.29}$$

If no v satisfies (6.28) then plainly $S_2 = 0$. Assume that (6.28) has a solution $v = v_0$ and take $I_1 = [v_0, v_0 + 2^{\lceil \frac{m-n}{2} \rceil - t - 2})$. Now any other v solving (6.29) must have

$$5^{vk} \equiv 5^{v_0 k} \bmod 2^{\lfloor \frac{m-n}{2} \rfloor} \Rightarrow vk \equiv v_0 k \bmod 2^{\lfloor \frac{m-n}{2} \rfloor - 2} \Rightarrow v \equiv v_0 \bmod 2^{\lfloor \frac{m-n}{2} \rfloor - t - 2}.$$

So if $m - n$ is even, I_1 contains only the solution v_0 and

$$S(A) = 2^{\lfloor \frac{m+n}{2} \rfloor + t} \chi_1(5^{v_0}) \chi_2(A 5^{v_0 k} + B). \tag{6.30}$$

Observe that a solution $x_0 = 5^{v_0}$ or $x_0 = -5^{v_0}$ of (6.25) corresponds to a solution v_0 to (6.28) when k is even and a solution v_0 to (6.28) for A or $-A$ respectively (both can not have solutions) if k is odd. The evaluation for S_2 follows at once from (6.30) and (6.26) or (6.27). When $m - n$ is odd, I_1 contains two solutions v_0 and $v_0 + 2^{\lfloor \frac{m-n}{2} \rfloor - t - 2}$ and

$$\begin{aligned} S(A) &= 2^{\lfloor \frac{m+n}{2} \rfloor + t} \chi_1(5^{v_0}) \left(\chi_2(h(5^{v_0})) + \chi_1(5^{2^{\lfloor \frac{m-n}{2} \rfloor - t - 2}}) \chi_2(A 5^{v_0 k} 5^{k 2^{\lfloor \frac{m-n}{2} \rfloor - t - 2}} + B) \right) \\ &= 2^{\lfloor \frac{m+n}{2} \rfloor + t} \chi_1(5^{v_0}) \chi_2(h(5^{v_0})) \left(1 + \chi_1(5^{2^{\lfloor \frac{m-n}{2} \rfloor - t - 2}}) \chi_2(\xi) \right) \end{aligned}$$

where, since $3\lfloor \frac{m-n}{2} \rfloor + n \geq m$ for $m \geq n + 3$,

$$\begin{aligned} \xi &= A 5^{v_0 k} \left(5^{k_1 2^{\lfloor \frac{m-n}{2} \rfloor - 2}} - 1 \right) h(5^{v_0})^{-1} + 1 \\ &= A 5^{v_0 k} h(5^{v_0})^{-1} \left((1 + R_{\lfloor \frac{m-n}{2} \rfloor} 2^{\lfloor \frac{m-n}{2} \rfloor})^{k_1} - 1 \right) + 1 \\ &\equiv A 5^{v_0 k} h(5^{v_0})^{-1} \left(k_1 R_{\lfloor \frac{m-n}{2} \rfloor} 2^{\lfloor \frac{m-n}{2} \rfloor} + \binom{k_1}{2} R^2_{\lfloor \frac{m-n}{2} \rfloor} 2^{m-n-1} \right) + 1 \bmod 2^m \\ &\equiv \left(A_1 5^{v_0 k} h(5^{v_0})^{-1} k_1 R_{\lfloor \frac{m-n}{2} \rfloor} R^{-1}_{\lfloor \frac{m+n}{2} \rfloor} + \frac{1}{2}(k_1 - 1) 2^{\lfloor \frac{m-n}{2} \rfloor} \right) R_{\lfloor \frac{m+n}{2} \rfloor} 2^{\lfloor \frac{m+n}{2} \rfloor} + 1 \bmod 2^m \\ &\equiv \left(1 + R_{\lfloor \frac{m+n}{2} \rfloor} 2^{\lfloor \frac{m+n}{2} \rfloor} \right)^{A_1 5^{v_0 k} h(5^{v_0})^{-1} k_1 R_{\lfloor \frac{m-n}{2} \rfloor} R^{-1}_{\lfloor \frac{m+n}{2} \rfloor} + \frac{1}{2}(k_1 - 1) 2^{\lfloor \frac{m-n}{2} \rfloor}} \bmod 2^m \\ &= 5^{\left(A_1 5^{v_0 k} h(5^{v_0})^{-1} k_1 R_{\lfloor \frac{m-n}{2} \rfloor} R^{-1}_{\lfloor \frac{m+n}{2} \rfloor} + \frac{1}{2}(k_1 - 1) 2^{\lfloor \frac{m-n}{2} \rfloor} \right) 2^{\lfloor \frac{m+n}{2} \rfloor - 2}}. \end{aligned}$$

Hence, setting

$$c_3 + c_2 A_1 5^{v_0 k} h (5^{v_0})^{-1} k_1 R_{\lceil \frac{m-n}{2} \rceil} R^{-1}_{\lceil \frac{m+n}{2} \rceil} = \lambda 2^{\lfloor \frac{m-n}{2} \rfloor}$$

(only the parity of λ will be used) and recalling that c_2 is odd, we have

$$\begin{aligned}\chi_1(5^{2^{\lfloor \frac{m-n}{2} \rfloor - t - 2}})\chi_2(\xi) &= e_{2^{\lceil \frac{m-n}{2} \rceil}} \left(c_3 + c_2 A_1 5^{v_0 k} h (5^{v_0})^{-1} k_1 R_{\lfloor \frac{m-n}{2} \rfloor} R^{-1}_{\lfloor \frac{m+n}{2} \rfloor} \right) (-1)^{\frac{1}{2}(k_1-1)c_2} \\ &= e_{2^{\lceil \frac{m-n}{2} \rceil}} \left(c_2 A_1 5^{v_0 k} h (5^{v_0})^{-1} k_1 \left(R_{\lfloor \frac{m-n}{2} \rfloor} R^{-1}_{\lfloor \frac{m+n}{2} \rfloor} - R_{\lceil \frac{m-n}{2} \rceil} R^{-1}_{\lceil \frac{m+n}{2} \rceil} \right) \right) (-1)^{\frac{1}{2}(k_1-1)+\lambda}.\end{aligned}$$

Since $1 + R_{i+1} 2^{i+1} = (1 + R_i 2^i)^2$ we have

$$R_{i+1} = R_i + 2^{i-1} R_i^2 \equiv R_i + 2^{i-1} \bmod 2^{i+2},$$

giving $R_i \equiv 3 \bmod 4$ for $i \geq 3$, and

$$\begin{aligned}&R_{\lfloor \frac{m-n}{2} \rfloor} R^{-1}_{\lfloor \frac{m+n}{2} \rfloor} - R_{\lceil \frac{m-n}{2} \rceil} R^{-1}_{\lceil \frac{m+n}{2} \rceil} \\ \equiv &R^{-1}_{\lfloor \frac{m+n}{2} \rfloor} R^{-1}_{\lceil \frac{m+n}{2} \rceil} \left((R_{\lceil \frac{m-n}{2} \rceil} - 2^{\lceil \frac{m-n}{2} \rceil - 2}) R_{\lceil \frac{m+n}{2} \rceil} - R_{\lceil \frac{m-n}{2} \rceil} (R_{\lceil \frac{m+n}{2} \rceil} - 2^{\lceil \frac{m-n}{2} \rceil + n - 2}) \right) \bmod 2^{\lceil \frac{m-n}{2} \rceil} \\ \equiv &(1 - 2^n) 2^{\lceil \frac{m-n}{2} \rceil - 2} \bmod 2^{\lceil \frac{m-n}{2} \rceil}.\end{aligned}$$

From (6.28) we have $c_2 A_1 5^{v_0 k} h (5^{v_0})^{-1} k_1 \equiv -c_3 \bmod 4$ and

$$S(A) = 2^{\lfloor \frac{m+n}{2} \rfloor + t} \chi_1(5^{v_0}) \chi_2(h(5^{v_0})) \left(1 + i^{(2^n-1)c_3} (-1)^{\frac{1}{2}(k_1-1)+\lambda} \right).$$

The result follows on writing

$$\frac{1 + i^h}{\sqrt{2}} = \omega^h \left(\frac{2}{h} \right).$$

6.3.3 Small m values: $t+2 \le m-n \le 2t+4$

Since $n+2(t+2) \ge m$ we have

$$\begin{aligned} A5^{\gamma k}+B &= A_1 2^n (1+R_{t+2}2^{t+2})^{\gamma k_1}+B \\ &\equiv (A+B)\left(1+\gamma k_1 A_1 R_{t+2}(A+B)^{-1}2^{t+n+2}\right) \bmod 2^m \\ &\equiv (A+B)\left(1+R_{t+n+2}2^{t+n+2}\right)^{\gamma k_1 A_1 (A+B)^{-1}R_{t+2}R_{t+n+2}^{-1}} \bmod 2^m \\ &= (A+B)5^{\gamma A k (A+B)^{-1}R_{t+2}R_{t+n+2}^{-1}}. \end{aligned}$$

Hence $\chi_1(5^\gamma)\chi_2(A5^{\gamma k}+B)$ equals

$$\chi_2(A+B)e_{2^{m-2}}\left(\gamma\left(c_1(A+B)+c_2 A k R_{t+2}R_{t+n+2}^{-1}\right)(A+B)^{-1}\right)$$

and $S(A)=2^{m-2}\chi_2(A+B)$ if $C(1)\equiv 0 \bmod 2^{m-2}$ and 0 otherwise. Since $m-n \ge t+2$ the congruence $C(1)\equiv 0 \bmod 2^{m-2}$ implies $c_1 = 2^{t+n}c_3$ (with c_3 odd if $m-n>t+2$) and becomes

$$c_3(A+B)+c_2 A_1 k_1 R_{t+2}R_{t+n+2}^{-1} \equiv 0 \bmod 2^{m-n-t-2}. \tag{6.31}$$

For $m-n=t+2$ or $t+3$ this will automatically hold (for both A and $-A$ when k is odd) and $S_2 = 2^{m-1}\chi_2(A+B)$ for k even and $\chi_1(-1)=1$, and

$$S_2 = 2^{m-2}(\chi_2(A+B)+\chi_1(-1)\chi_2(-A+B))$$

for k odd. Further for k odd and $m-n=2$ we have $-A+B \equiv (1+2^{m-1})(A+B) \bmod 2^m$ with $\chi_2(1+2^{m-1})=-1$ and $S_2 = 2^{m-2}\chi_2(A+B)(1-\chi_1(-1)) = 2^{m-1}\chi_2(A+B)$ if $\chi_1(-1)=-1$ and zero otherwise. Note when $m-n=t+2$ we have $c_1=2^{m-2}$ and $\chi_1(5)=1$ and when $m-n=t+3$ we have $c_1=2^{m-2}$ or 2^{m-3} and $\chi_1(5)=\pm 1$.

Since $c_3 B$ is odd (6.31) can not hold for both A and $-A$ for $m-n>t+3$ and thus at most one of $S(A)$ or $S(-A)$ is non-zero. When k is odd the congruence condition for $-A$

becomes $C(-1) \equiv 0 \bmod 2^{m-2}$.

Chapter 7

Evaluating Jacobi Sums

For multiplicative characters χ_1 and χ_2 mod q one defines the classical Jacobi sum by

$$J(\chi_1, \chi_2, q) := \sum_{x=1}^{q} \chi_1(x)\chi_2(1-x). \tag{7.1}$$

More generally for k characters $\chi_1, \ldots, \chi_k$ mod q one can define

$$J(\chi_1, \ldots, \chi_k, q) = \sum_{x_1=1}^{q} \cdots \sum_{\substack{x_k=1 \\ x_1+\cdots+x_k=1}}^{q} \chi_1(x_1)\cdots\chi_k(x_k). \tag{7.2}$$

If the χ_i are mod rs characters with $(r,s)=1$ then, writing $\chi_i = \chi_i'\chi_i''$ where χ_i' and χ_i'' are mod r and mod s characters respectively, as we have discussed in Section 2.2

$$J(\chi_1, \ldots, \chi_k, rs) = J(\chi_1', \ldots, \chi_k', r)J(\chi_1'', \ldots, \chi_k'', s).$$

Hence, it suffices to consider the case of prime power moduli $q = p^m$.

Zhang & Yao [30] showed that the sums (7.1) can in fact be evaluated explicitly when m is even (and χ_1, χ_2 and $\chi_1\chi_2$ are primitive mod p^m). Working with a slightly more general binomial character sum the authors [21] showed that techniques of Cochrane & Zheng [4]

can be used to obtain an evaluation of (7.1) for any $m > 1$ (p an odd prime). Zhang and Xu [32] considered the general case, (7.2), obtaining (assuming that $\chi, \chi^{n_1}, \dots, \chi^{n_k}$, and $\chi^{n_1+\cdots+n_k}$ are primitive characters modulo p^m)

$$J(\chi^{n_1}, \dots, \chi^{n_k}, p^m) = p^{\frac{1}{2}(k-1)m}\overline{\chi}(u^u)\chi(n_1^{n_1}\dots n_k^{n_k}), \quad u := n_1 + \cdots + n_k, \tag{7.3}$$

when m is even, and when the $m, k, n_1, \dots, n_k$ are all odd

$$J(\chi^{n_1}, \dots, \chi^{n_k}, p^m) = p^{\frac{1}{2}(k-1)m}\overline{\chi}(u^u)\chi(n_1^{n_1}\dots n_{k-1}^{n_{k-1}}) \begin{cases} \varepsilon_p^{k-1}\left(\frac{un_1\dots n_k}{p}\right), & \text{if } p \neq 2; \\ \left(\frac{2}{un_1\dots n_k}\right) & \text{if } p = 2, \end{cases} \tag{7.4}$$

where $\left(\frac{m}{n}\right)$ is the Jacobi symbol and (defined more generally for later use)

$$\varepsilon_{p^m} := \begin{cases} 1, & \text{if } p^m \equiv 1 \bmod 4, \\ i, & \text{if } p^m \equiv 3 \bmod 4. \end{cases} \tag{7.5}$$

In this Chapter, representing joint work with M. Long and C. Pinner [15], we give an evaluation for all $m > 1$ (i.e. irrespective of the parity of k and the n_i). In fact, we evaluate the slightly more general sum

$$J_B(\chi_1, \dots, \chi_k, p^m) = \sum_{x_1=1}^{p^m} \cdots \sum_{\substack{x_k=1 \\ x_1+\cdots+x_k=B}}^{p^m} \chi_1(x_1)\cdots\chi_k(x_k).$$

Of course when $B = p^n B'$, $p \nmid B'$ the simple change of variables $x_i \mapsto B'x_i$ gives

$$J_B(\chi_1, \dots, \chi_k, p^m) = \chi_1\cdots\chi_k(B')J_{p^n}(\chi_1, \dots, \chi_k, p^m).$$

For example $J_B(\chi_1, \dots, \chi_k, p^m) = \chi_1\cdots\chi_k(B)J(\chi_1, \dots, \chi_k, p^m)$ when $p \nmid B$. From the

change of variables $x_i \mapsto -x_k x_i$, $1 \le i < k$ one also sees that

$$J_{p^m}(\chi_1, \dots, \chi_k, p^m) = \begin{cases} \phi(p^m)\chi_k(-1)J(\chi_1, \dots, \chi_{k-1}, p^m), & \text{if } \chi_1 \cdots \chi_k = \chi_0, \\ 0, & \text{if } \chi_1 \cdots \chi_k \neq \chi_0, \end{cases}$$

where χ_0 denotes the principal character, so we assume that $B = p^n$ with $n < m$.

Theorem 7.0.1. *Let p be a prime and $m \ge n+2$. Suppose that $\chi_1, \dots, \chi_k$ are $k \ge 2$ characters mod p^m with at least one of them primitive.*

If the $\chi_1, \dots, \chi_k$ are not all primitive mod p^m or $\chi_1 \dots \chi_k$ is not induced by a primitive mod p^{m-n} character, then $J(\chi_1, \dots, \chi_k, p^m) = 0$.

If the $\chi_1, \dots, \chi_k$ are primitive mod p^m and $\chi_1 \cdots \chi_k$ is primitive mod p^{m-n}, then

$$J_{p^n}(\chi_1, \dots, \chi_k, p^m) = p^{\frac{1}{2}(m(k-1)+n)} \frac{\chi_1(c_1) \cdots \chi_k(c_k)}{\chi_1 \cdots \chi_k(v)}\, \delta, \tag{7.6}$$

where for p odd

$$\delta = \left(\frac{-2r}{p}\right)^{m(k-1)+n} \left(\frac{v}{p}\right)^{m-n} \left(\frac{c_1 \cdots c_k}{p}\right)^{m} \varepsilon_{p^m}^{k} \varepsilon_{p^{m-n}}^{-1},$$

and for $p = 2$ and $m - n \ge 5$,

$$\delta = \left(\frac{2}{v}\right)^{m-n} \left(\frac{2}{c_1 \cdots c_k}\right)^{m} \omega^{(2^n-1)v}, \tag{7.7}$$

with ε_{p^m} as defined in (7.5), the r and c_i as in (2.8) and (2.10) or (2.12), and

$$v := p^{-n}(c_1 + \cdots + c_k), \quad \omega := e^{\pi i/4}. \tag{7.8}$$

Of course it is natural to assume that at least one of the $\chi_1, \dots, \chi_k$ is primitive, otherwise we can reduce the sum to a mod p^{m-1} sum. For $n = 0$ and $\chi_1, \dots, \chi_k$ and $\chi_1 \cdots \chi_k$ all

primitive mod p^m our result simplifies to

$$J(\chi_1,\dots,\chi_k,p^m) = p^{\frac{m(k-1)}{2}}\frac{\chi_1(c_1)\cdots\chi_k(c_k)}{\chi_1\cdots\chi_k(v)}\,\delta, \quad v = c_1+\cdots+c_k,$$

with

$$\delta = \begin{cases} 1, & \text{if } m \text{ is even,} \\ \left(\frac{vc_1\cdots c_k}{p}\right)\left(\frac{-2rc}{p}\right)^{k-1}\varepsilon_p^{k-1}, & \text{if } m \text{ is odd and } p\neq 2, \\ \left(\frac{2}{vc_1\cdots c_k}\right), & \text{if } m\geq 5 \text{ is odd and } p=2. \end{cases}$$

In the remaining $n=0$ case, $p=2$, $m=3$ we have $J(\chi_1,\dots,\chi_k,2^3) = 2^{\frac{3}{2}(k-1)}(-1)^{\lfloor\frac{\ell}{2}\rfloor}$ where ℓ denotes the number of characters $1\leq i\leq k$ with $\chi_i(-1)=-1$.

When the $\chi_i=\chi^{n_i}$ for some primitive mod p^m character χ we can write $c_i=n_ic$ (where c is determined by $\chi(a)$ as in (2.10) or (2.12)) and we recover the form (7.3) and (7.4) with the addition of a factor $\left(\frac{-2rc}{p}\right)^{k-1}$ for $p\neq 2$, m odd, which of course can be ignored when k is odd as assumed in [32].

For completeness we observe that in the few remaining $m\geq n+2$ cases (7.6) becomes

$$J_{p^n}(\chi_1,\dots,\chi_k,p^m) = 2^{\frac{1}{2}(m(k-1)+n)}\begin{cases} -i\omega^{k-\sum_{i=1}^k\chi_i(-1)}, & \text{if } m=3,\ n=1, \\ \omega^{\chi_1\cdots\chi_k(-1)-1-v}\prod_{i=1}^k\chi_i(-c_i), & \text{if } m=4,\ n=1, \\ i^{1-v}\prod_{i=1}^k\chi_i(c_i), & \text{if } m=4,\ n=2. \end{cases}$$

For $m=n+1$ (with at least one χ_i primitive) the Jacobi sum is still zero unless all the χ_i are primitive mod p^m and $\chi_1\cdots\chi_k$ is a mod p character. Then we can say that $|J_{p^n}(\chi_1,\dots,\chi_k,p^m)| = p^{\frac{1}{2}mk-1}$ if $\chi_1\cdots\chi_k=\chi_0$ and $p^{\frac{1}{2}(mk-1)}$ otherwise, but an explicit evaluation in the latter case is equivalent to an explicit evaluation of the mod p Gauss sum $G(\chi_1\cdots\chi_k,p)$ when $m\geq 2$. We saw in Section 4.4 that if χ_k is a primitive mod p^m character

and $\chi_1 \cdots \chi_k$ is a mod p^{m-n} character we can write

$$J_{p^n}(\chi_1, \dots, \chi_k, p^m) = p^n \frac{\overline{G(\chi_1 \cdots \chi_k, p^{m-n})}}{\overline{G(\chi_k, p^m)}} \prod_{i=1}^{k-1} G(\chi_i, p^m).$$

We will use this and the explicit evaluation of the Gauss sums in Theorem 3.1.1 to evaluate the sum.

7.1 Proof of Theorem 7.0.1

We assume that $\chi_1, \dots, \chi_k$ are all primitive mod p^m characters and $\chi_1 \cdots \chi_k$ is a primitive mod p^{m-n} character, since otherwise from Theorem 4.4.1 and (4.18), $J_{p^n}(\chi_1, \dots, \chi_k, p^m) = 0$. In particular we have (4.19).

Writing $R = R_{\lceil \frac{m}{2} \rceil + 2}$ then by (4.19) and the evaluation of Gauss sums in Theorem 3.1.1 we have

$$\begin{aligned} J_{p^n}(\chi_1, \dots, \chi_k, p^m) &= \frac{\prod_{i=1}^k G(\chi_i, p^m)}{G(\chi_1 \cdots \chi_k, p^{m-n})} \\ &= \frac{\prod_{i=1}^k p^{m/2} \chi_i(-c_i R^{-1}) e_{p^m}(-c_i R^{-1}) \delta_i}{p^{(m-n)/2} \chi_1 \cdots \chi_k(-vR^{-1}) e_{p^{m-n}}(-vR^{-1}) \delta_s} \\ &= p^{\frac{1}{2}(m(k-1)+n)} \frac{\prod_{i=1}^k \chi_i(c_i)}{\chi_1 \cdots \chi_k(v)} \delta_s^{-1} \prod_{i=1}^k \delta_i, \end{aligned} \tag{7.9}$$

where $p^n v = c_1 + \cdots + c_k$,

$$\delta_i = \begin{cases} \left(\frac{-2rc_i}{p}\right)^m \varepsilon_{p^m}, & \text{if } p \text{ is odd, } p \neq 2, \\ \left(\frac{2}{c_i}\right)^m \omega^{c_i}, & \text{if } p = 2 \text{ and } m \geq 5, \end{cases}$$

and

$$\delta_s = \begin{cases} \left(\frac{-2rv}{p}\right)^{m-n} \varepsilon_{p^{m-n}}, & \text{if } p \text{ is odd,} \\ \left(\frac{2}{v}\right)^{m-n} \omega^v, & \text{if } p = 2 \text{ and } m-n \geq 5, \end{cases}$$

and the result is plain when p is odd or $p = 2$, $m - n \geq 5$.

The remaining cases $p = 2$, $m \geq 5$ and $m - n = 2, 3, 4$, follows similarly using the adjustment to δ_s observed at the end of the proof of Theorem 3.1.1 .

7.2 A more direct approach

We should note that the Cochrane & Zheng reduction technique [4] can be applied to directly evaluate the Jacobi sums when p is odd and $m \geq n + 2$ instead of using the Gauss sum evaluation. For example if $b = p^n b'$ with $p \nmid b'$, then from [21, Theorem 3.1] we have

$$\begin{aligned} J_b(\chi_1, \chi_2, p^m) &= \sum_{x=1}^{p^m} \chi_1(x)\chi_2(b-x) = \sum_{x=1}^{p^m} \overline{\chi_1\chi_2}(x)\chi_2(bx-1) \\ &= p^{\frac{m+n}{2}} \overline{\chi_1\chi_2}(x_0)\chi_2(bx_0-1)\left(\frac{-2c_2rb'x_0}{p}\right)^{m-n} \varepsilon_{p^{m-n}}, \end{aligned}$$

where x_0 is a solution to the characteristic equation

$$c_1 + c_2 - c_1 bx \equiv 0 \bmod p^{\lfloor \frac{m+n}{2} \rfloor + 1}, \quad p \nmid x(bx-1). \tag{7.10}$$

If (7.10) has no solution mod $p^{\lfloor \frac{m+n}{2} \rfloor}$ then $J_b(\chi_1, \chi_2, p^m) = 0$. In particular we see that:

i. If $p \nmid c_1$ and $p \mid c_2$, then $J_b(\chi_1, \chi_2, p^m) = 0$.

ii. If $p \nmid c_1 c_2 (c_1 + c_2)$ then

$$J_b(\chi_1, \chi_2, p^m) = \chi_1\chi_2(b)\chi_1(c_1)\chi_2(c_2)\overline{\chi_1\chi_2}(c_1+c_2)p^{\frac{m}{2}}\delta_2.$$

where

$$\delta_2 = \left(\frac{-2r}{p}\right)^m \left(\frac{c_1c_2(c_1+c_2)}{p}\right)^m \varepsilon_{p^m}.$$

iii. If $p \nmid c_1$ and $b = p^n b'$, $p \nmid b'$ with $n < m-1$ then $J_b(\chi_1, \chi_2, p^m) = 0$ unless $p^n \mid\mid (c_1+c_2)$ in which case writing $w = (c_1+c_2)/p^n$,

$$J_b(\chi_1, \chi_2, p^m) = \chi_1\chi_2(b')\frac{\chi_1(c_1)\chi_2(c_2)}{\chi_1\chi_2(w)} p^{\frac{m+n}{2}} \left(\frac{-2r}{p}\right)^{m-n} \left(\frac{c_1c_2w}{p}\right)^{m-n} \varepsilon_{p^{m-n}}.$$

To see (ii) observe that if $p \mid b$, then $J_b(\chi_1, \chi_2, p^m) = 0$, and if $p \nmid b$, then we can take $x_0 \equiv (c_1+c_2)c_1^{-1}b^{-1} \bmod p^m$ (and hence $bx_0 - 1 = c_2c_1^{-1}$). Similarly for (iii) if $p^n \mid\mid (c_1+c_2)$ we can take $x_0 \equiv p^{-n}(c_1+c_2)c_1^{-1}(b')^{-1} \bmod p^m$.

Of course we can write the generalized sum in the form

$$\begin{aligned} J_{p^n}(\chi_1, \dots, \chi_k) &= \sum_{x_3=1}^{p^m} \cdots \sum_{x_k=1}^{p^m} \chi_3(x_3)\dots\chi_k(x_k) \sum_{\substack{x_1=1 \\ b:=p^n-x_3-\cdots-x_k}}^{p^m} \chi_1(x_1)\chi_2(b-x_1) \\ &= \sum_{x_3=1}^{p^m} \cdots \sum_{x_k=1}^{p^m} \chi_3(x_3)\dots\chi_k(x_k) J_b(\chi_1, \chi_2, p^m), \end{aligned}$$

Hence assuming that at least one of the χ_i is primitive mod p^m (and reordering the characters as necessary) we see from (i) that $J_{p^n}(\chi_1, \dots, \chi_k, p^m) = 0$ unless all the characters are primitive mod p^m. Also when $k = 2$, χ_1, χ_2 primitive, we see from (iii) that $J_{p^n}(\chi_1, \chi_2, p^m) = 0$ unless $\chi_1\chi_2$ is induced by a primitive mod p^{m-n} character, in which case we recover the formula in Theorem 7.0.1 on observing that $\left(\frac{c_1c_2}{p}\right)^n \varepsilon_{p^{m-n}}^2 = \varepsilon_{p^m}^2$; this is plain when n is even, for n odd observe that $\left(\frac{c_1c_2}{p}\right) = \left(\frac{(c_1+c_2)^2-(c_1-c_2)^2}{p}\right) = \left(\frac{-1}{p}\right)$, (since $p \mid (c_1+c_2)$ as $\chi_1\chi_2$ is imprimitive). We show that a simple induction recovers the formula for all $k \geq 3$. We assume that all the χ_i are primitive mod p^m and observe that when $k \geq 3$ we can further assume (reordering as necessary) that $\chi_1\chi_2$ is also primitive mod p^m, since if $\chi_1\chi_3$, $\chi_2\chi_3$ are not primitive then $p \mid (c_1+c_3)$ and $p \mid (c_2+c_3)$ and $(c_1+c_2) \equiv -2c_3 \not\equiv 0 \bmod p$ and $\chi_1\chi_2$

is primitive. Hence from (ii) we can write

$$J_{p^m}(\chi_1,\dots,\chi_k,p^m)=\frac{\chi_1(c_1)\chi_2(c_2)}{\chi_1\chi_2(c_1+c_2)}p^{\frac{m}{2}}\delta_2\sum_{x_3=1}^{p^m}\cdots\sum_{x_k=1}^{p^m}\chi_3(x_3)\dots\chi_k(x_k)\chi_1\chi_2(b)$$

$$=\chi_1(c_1)\chi_2(c_2)\overline{\chi_1\chi_2}(c_1+c_2)p^{\frac{m}{2}}\delta_2 J_{p^n}(\chi_1\chi_2,\chi_3,\dots,\chi_k,p^m).$$

Assuming the result for $k-1$ characters we have $J_{p^n}(\chi_1\chi_2,\chi_3,\dots,\chi_k,p^m)=0$ unless $\chi_1\cdots\chi_k$ is induced by a primitive mod p^{m-n} character in which case

$$J_{p^n}(\chi_1\chi_2,\chi_3,\dots,\chi_k,p^m)=\chi_1\chi_2(c_1+c_2)\prod_{i=3}^{k}\chi_i(c_i)\overline{\chi_1\dots\chi_k}(v)\delta_3 p^{\frac{m(k-2)+n}{2}}$$

with

$$\delta_3=\left(\frac{-2r}{p}\right)^{m(k-2)+n}\left(\frac{v}{p}\right)^{m-n}\left(\frac{(c_1+c_2)c_3\dots c_k}{p}\right)^{m}\varepsilon_{p^m}^{k-1}\varepsilon_{p^{m-n}}^{-1}.$$

Our formula for k characters then follows on observing that $\delta_2\delta_3=\delta$.

Bibliography

[1] T. Apostol, *Introduction to Analytic Number Theory*, Springer 1976.

[2] B. C. Berndt, R. J. Evans & K. S. Williams, *Gauss and Jacobi Sums*, Canadian Math. Soc. series of monographs and advanced texts, vol. 21, Wiley, New York 1998.

[3] F. Castro & C. Moreno, *Mixed exponential sums over finite fields*, Proc. Amer. Math. Soc. 128 (2000), 2529-2537.

[4] T. Cochrane, Zhiyong Zheng, *Pure and mixed exponential sums*, Acta Arith. 91 (1999), no. 3, 249-278.

[5] T. Cochrane, Zhiyong Zheng, *A survey on pure and mixed exponential sums modulo prime powers*, Number theory for the millennium, I (Urbana, IL, 2000), 273-300, A. K. Peters, Natick, MA, 2002.

[6] T. Cochrane, *Exponential sums modulo prime powers*, Acta Arith. 101 (2002), no. 2, 131-149.

[7] T. Cochrane, *Exponential sums with rational function entries*, Acta Arith. 95 (2000), no. 1, 67-95

[8] T. Cochrane and C. Pinner, *Using Stepanov's method for exponential sums involving rational functions*, J. Number Theory 116 (2006), no. 2, 270-292.

[9] T. Cochrane *Exponential sums modulo prime powers*, Acta Arith. 101 (2002), no. 2, 131-149.

[10] Han Di, *A hybrid mean value involving two-term exponential sums and polynomial character sums*, to appear Czech. Math. J.

[11] D. R. Heath-Brown, *An estimate for Heilbronn's exponential sum*, Analytic Number Theory: Proceedings of a conference in honor of Heini Halberstam, Birkhäuser, Boston, MA, (1996), 451-463.

[12] D. R. Heath-Brown and S. Konyagin, *New bounds for Gauss sums derived from kth powers, and for Heilbronn's exponential sum*, Quart. J. Math. 51 (2000), 221-235.

[13] P. Leonard & K. Williams, *Evaluation of certain Jacobsthal sums*, Boll. Unione Mat. Ital. 15 (1978), 717-723.

[14] R. Lidl & H. Niederreiter, *Finite Fields*, Encyclopedia of Mathematics and its applications 20, 2nd edition, Cambridge University Press, 1997.

[15] M. Long, V. Pigno & C. Pinner, *Evaluating Prime Power Gauss and Jacobi Sums*, submitted Rocky Mountain J. Math. (http://www.math.ksu.edu/∼ pinner/research.html preprint 39.)

[16] J.-L. Mauclaire, *Sommes de Gauss modulo p^α, I & II*, Proc. Japan Acad. Ser. A 59 (1983), 109-112 & 161-163.

[17] L. J. Mordell, *On Salié's sum*, Glasgow Math. J. 14 (1973), 25-26.

[18] I. Niven, H.S. Zuckerman & H. L. Montgomery *An Introduction to The Theory of Numbers*, 5th edition, John Wiley & Sons, Inc. 1991.

[19] R. Odoni, *On Gauss sums (mod p^n), $n \geq 2$*, Bull. London Math. Soc. 5 (1973), 325-327.

[20] V. Pigno & C. Pinner, *Twisted monomial Gauss sums modulo prime powers*, to appear Funct. Approx. Comment. Math.

[21] V. Pigno & C. Pinner, *Binomial Character Sums Modulo Prime Powers*, submitted to Journal de Théor. Nombres Bordeaux.

[22] V. Pigno, C. Pinner & J. Sheppard, *Evaluating Binomial Character Sums Modulo Powers of Two*, submitted to J. Math. Appl. (http://www.math.ksu.edu/∼ pinner/research.html preprint 40.)

[23] J-C. Puchta, *Remark on a paper of Yu on Heilbronn's exponential sum*, J. Number Theory 87 (2001), 239-241.

[24] A. Weil, *On some exponential sums*, Proc. Nat. Acad. Sci. U.S.A. 34 (1948), 203-210.

[25] Hans Salié, *Uber die Kloostermanschen summen* $S(u, v; q)$, Math. Zeit. 34 (1931-32), 91-109.

[26] X. Guo and T. Wang, *On the generalized k-th Gauss sums*, to appear Hacet. J. Math. Stat.

[27] K. Williams, *On Salié's sum*, J. Number Theory 3 (1971), 316-317.

[28] K. Williams, *Note on Salié's sum*, Proc. Amer. Math. Soc., Vol 30, no. 2 (1971), 393-394.

[29] Y. He and W. Zhang, *On the* $2k$*-th power mean value of the generalized quadratic Gauss sum*, Bull Korean Math. Soc. 48 (2011), 9-15.

[30] W. Zhang & W. Yao, *A note on the Dirichlet characters of polynomials*, Acta Arith. 115 (2004), no. 3, 225-229.

[31] W. Zhang & Y. Yi, *On Dirichlet Characters of Polynomials*, Bull. London Math. Soc. 34 (2002), no. 4, 469-473.

[32] W. Zhang & Z. Xu, *On the Dirichlet characters of polynomials in several variables*, Acta Arith. 121 (2006), no. 2, 117-124.

[33] J. Wang, *On the Jacobi sums mod* P^n, J. Number Theory 39 (1991), 50-64.

[34] F. Liu and Q.-H. Yang, *An identity on the* $2m$*-th power mean value of the generalized Gauss sums*, Bull. Korean Math. Soc. 49 (2012), no. 6, 1327-1334.

[35] Yu. V. Malykhin, *Bounds for exponential sums modulo* p^2, Journal of Mathematical Sciences, 146, No. 2, (2007), 5686-5696 [Translated from Fundamentalnaya i Prikladnaya Matematika, 11, No. 6, (2005), 81-94].

[36] Yu. V. Malykhin, *Estimates of trigonometric sums modulo* p^r, Mathematical Notes 80 (2006), No. 5, 748-752. [Translated from Matematicheskie Zametki 80 (2006), No. 5, 793-796].

[37] W. Zhang and H. Liu, *On the general Gauss sums and their fourth power means*, Osaka J. Math. 42 (2005), 189-199.