GENERALIZED JACOBI SUMS MODULO PRIME POWERS

by

BADRIA ALSULMI

B.S., King Abdulaziz University, 2004

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

2016

Abstract

For mod p Dirichlet characters χ_1, χ_2 the classical Jacobi sums

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

have a long history in number theory. In particular, it is well known that if χ_1, χ_2 and $\chi_1\chi_2$ are non-trivial characters, then $J(\chi_1, \chi_2, p)$ can be written in terms of Gauss sums and

$$|J(\chi_1, \chi_2, p)| = p^{1/2},$$

though in general no evaluation is known without the absolute value. In this thesis we consider some mod p^m generalization of the Jacobi sums where we can obtain an explicit evaluation (without the absolute value) for m sufficiently large. For example, if $\chi, \chi_1, \cdots, \chi_s$ are mod p^m Dirichlet characters the sums

$$\mathcal{J}_1 = \sum_{\substack{x_1=1 \\ A_1x_1^{k_1}+\cdots+A_sx_s^{k_s}\equiv B \bmod p^m}}^{p^m} \cdots \sum_{x_s=1}^{p^m} \chi_1(x_1)\cdots\chi_s(x_s),$$

where $p \nmid A_1 \cdots A_s \, B \, k_1 \cdots k_s$, and

$$\mathcal{J}_2 = \sum_{x_1=1}^{p^m} \cdots \sum_{x_s=1}^{p^m} \chi_1(x_1)\cdots\chi_s(x_s)\chi(A_1x_1 + \cdots + A_sx_s + Bx_1^{w_1}\cdots x_s^{w_s}),$$

where $p \nmid 2A_1 \cdots A_s B(1 - w_1 - \cdots - w_s)$, have simple evaluations when $m \geq 2$. Exponential or character sums with an explicit evaluation are rare. Interestingly the sums we consider here can, like the classical Jacobi sums, be written in terms of Gauss sums.

GENERALIZED JACOBI SUMS MODULO PRIME POWERS

by

BADRIA ALSULMI

B.S., King Abdulaziz University, 2004

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

2016

Approved by:

Major Professor
Christopher Pinner

Abstract

For mod p Dirichlet characters χ_1, χ_2 the classical Jacobi sums

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

have a long history in number theory. In particular, it is well known that if χ_1, χ_2 and $\chi_1\chi_2$ are non-trivial characters, then $J(\chi_1, \chi_2, p)$ can be written in terms of Gauss sums and

$$|J(\chi_1, \chi_2, p)| = p^{1/2},$$

though in general no evaluation is known without the absolute value. In this thesis we consider some mod p^m generalization of the Jacobi sums where we can obtain an explicit evaluation (without the absolute value) for m sufficiently large. For example, if $\chi, \chi_1, \cdots, \chi_s$ are mod p^m Dirichlet characters the sums

$$\mathcal{J}_1 = \sum_{\substack{x_1=1 \\ A_1x_1^{k_1}+\cdots+A_sx_s^{k_s}\equiv B \bmod p^m}}^{p^m} \cdots \sum_{x_s=1}^{p^m} \chi_1(x_1)\cdots\chi_s(x_s),$$

where $p \nmid A_1 \cdots A_s\, B\, k_1 \cdots k_s$, and

$$\mathcal{J}_2 = \sum_{x_1=1}^{p^m} \cdots \sum_{x_s=1}^{p^m} \chi_1(x_1)\cdots\chi_s(x_s)\chi(A_1x_1 + \cdots + A_sx_s + Bx_1^{w_1}\cdots x_s^{w_s}),$$

where $p \nmid 2A_1 \cdots A_sB(1 - w_1 - \cdots - w_s)$, have simple evaluations when $m \geq 2$. Exponential or character sums with an explicit evaluation are rare. Interestingly the sums we consider here can, like the classical Jacobi sums, be written in terms of Gauss sums.

Table of Contents

List of Tables

Acknowledgments

Foremost, I would like to thank the God for everything. Many thanks go to my advisor Professor Chris Pinner for his supports and his encouragements. Thank you for giving me your time and helping me go through the hard way with constant encouragement. Your suggestions made this work successful. Thank you for your patience with me. Also, I would like to thank my colleague Vincent Pigno, who jointed this work with me.

I would like to thank my committee members, Professor Todd Cochrane and Professor Craig Spencer for their continuous support and their guidances that helped me all the time.

Thank you to Misty Ostergaard for being such a wonderful friend. You brings the smile to me every time I see you. We have had great conversations whether related to Math or to life in general.

Finally, I would like to thank my husband Asim for his support and patient, my brother Amar, who encouraged me to come to K-State where the place he graduated from, and my entire family. Thanks to my kids, my daughter Soso and my baby boy Rayan.

Dedication

This thesis is dedicated to my father's soul, who passed away in 2011. He asked me for a promise to get my Ph.D, and I did.

Chapter 1

Introduction

Exponential and character sums are used frequently in number theory so it is always interesting when such a sum has an explicit evaluation. For example, for a non-trivial mod p character χ the classical Gauss sums

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

where $e_k(x) := e^{2\pi i x/k}$, satisfy

$$|G(\chi, p)| = p^{1/2},$$

with an evaluation of $G(\chi, p)$ famously obtained by Gauss in the special case that $\chi(x)$ is the Legendre symbol. Another much studied sum is the Jacobi sum, mentioned by Jacobi [10] in a letter to Gauss dated February 8, 1827. For two characters χ_1, χ_2 mod p one defines

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

An extensive history of Jacobi sums and their applications can be found in [4, Chapter 2] and [11, Chapter 5]. It is well known that if $\chi_1\chi_2$ is a non-trivial character, then $J(\chi_1, \chi_2, p)$

can be written in terms of Gauss sums

$$J(\chi_1, \chi_2, p) = \frac{G(\chi_1, p)G(\chi_2, p)}{G(\chi_1\chi_2, p)},$$

and hence if χ_1, χ_2 and $\chi_1\chi_2$ are non-trivial

$$|J(\chi_1, \chi_2, p)| = p^{1/2}.$$

These have natural generalization to characters on finite fields $\mathbb{F}_{p^m}$ and to sums with more than two characters (see [4, Theorem 2.1.3] and [11, Theorem 5.21]). For example, if $\chi_1, \dots, \chi_s$ are mod p characters, we can define

$$J(\chi_1, \dots, \chi_s, p) := \sum_{\substack{x_1=1 \\ x_1+\cdots+x_s\equiv 1 \bmod p}}^{p} \cdots \sum_{x_s=1}^{p} \chi_1(x_1)\cdots\chi_s(x_s). \tag{1.1}$$

If $\chi_1 \cdots \chi_s$ is non-trivial, then we can write (1.1) in the form

$$J(\chi_1, \dots, \chi_s, p) = \frac{\prod_{i=1}^{s} G(\chi_i, p)}{G(\chi_1\cdots\chi_s, p)},$$

and if $\chi_1, \dots, \chi_s, \chi_1 \dots \chi_s$ are non-trivial characters, then

$$|J(\chi_1, \dots, \chi_s, p)| = p^{\frac{s-1}{2}}.$$

Here we are interested in working in the ring $\mathbb{Z}_{p^m}$ rather than the finite field $\mathbb{F}_{p^m}$. When $\chi_1, \dots, \chi_s$, are mod p^m Dirichlet characters one can similarly define the Jacobi sums

$$J(\chi_1, \dots, \chi_s, p^m) := \sum_{\substack{x_1=1 \\ x_1+\cdots+x_s\equiv 1 \bmod p^m}}^{p^m} \cdots \sum_{x_s=1}^{p^m} \chi_1(x_1)\cdots\chi_s(x_s). \tag{1.2}$$

These had already been considered for $s = 2$ by Zhang and Yao [24] and for general s by Zhang and Xu [23] who obtained a Gauss sum decomposition

$$J(\chi_1, \ldots, \chi_s, p^m) = \frac{\prod_{i=1}^{s} G(\chi_i, p^m)}{G(\chi_1 \cdots \chi_s, p^m)},$$

where

$$G(\chi, p^m) := \sum_{x=1}^{p^m} \chi(x) e_{p^m}(x), \tag{1.3}$$

under the assumption that the $\chi_1, \ldots, \chi_s$, and $\chi_1 \cdots \chi_s$ are all primitive characters, and hence

$$|J(\chi_1, \ldots, \chi_s, p^m)| = p^{\frac{(s-1)m}{2}},$$

(see also Lemma 1 in [25]). Wang [20] had already obtained such an expression for Jacobi sums over much more general rings of residues modulo prime powers and related the number of solutions of the congruence $x_1^p + \cdots + x_s^p \equiv 1 \bmod p^2$ to the number of certain real Jacobi sums over rings. Jacobi sums over finite local rings can be found in Wang [21]. A slightly more general sum

$$J_B(\chi_1, \ldots, \chi_s, p^m) := \sum_{\substack{x_1=1 \\ x_1+\cdots+x_s \equiv B \bmod p^m}}^{p^m} \cdots \sum_{x_s=1}^{p^m} \chi_1(x_1) \cdots \chi_s(x_s), \tag{1.4}$$

was evaluated in [15]. While mod p sums are usually difficult to evaluate, the method of Cochrane and Zheng [7] can sometimes be used to evaluate mod p^m sums when $m \geq 2$, as formulated in [17]. This technique was for instance used in [7, §9] to explicitly evaluate the Gauss sums (1.3) for $m \geq 2$. Slightly different evaluations can be found in [14], [12] and [15]. In [15] the Jacobi sums (1.4) were written in terms of Gauss sums and the Gauss sum evaluation used to obtain an evaluation of the Jacobi sums for $m \geq 2$ (see (3.10) in Chapter 3).

Here we are interested in two different generalizations of the Jacobi sums (1.4) where we can also obtain an explicit evaluation. For example, if $\chi, \chi_1, \cdots, \chi_s$ are mod p^m Dirichlet characters the following Jacobi sums

$$\mathcal{J}_1 := \sum_{\substack{x_1=1 \\ A_1 x_1^{k_1}+\cdots+A_s x_s^{k_s} \equiv B \bmod p^m}}^{p^m} \cdots \sum_{x_s=1}^{p^m} \chi_1(x_1)\cdots\chi_s(x_s), \tag{1.5}$$

where

$$p \nmid A_1 \cdots A_s B k_1 \cdots k_s, \tag{1.6}$$

and

$$\mathcal{J}_2 := \sum_{x_1=1}^{p^m} \cdots \sum_{x_s=1}^{p^m} \chi_1(x_1)\cdots\chi_s(x_s)\chi(A_1x_1+\cdots+A_sx_s+Bx_1^{w_1}\cdots x_s^{w_s}), \tag{1.7}$$

where

$$p \nmid 2A_1\cdots A_s B(1-w_1-\cdots-w_s), \tag{1.8}$$

have simple evaluations when $m \geq 2$. Of course, the classical Jacobi sums (1.4) correspond to taking all the $A_i = 1$ and $k_i = 1$ in $\mathcal{J}_1$, and all the $w_i = 0$ in $\mathcal{J}_2$.

The following evaluation of $\mathcal{J}_1$ is a special case of Theorem 3.0.2 which we shall prove in Chapter 3. For simplicity, we have stated the result here for $|\mathcal{J}_1|$, but in fact we obtain an evaluation for $\mathcal{J}_1$. The condition (1.6) can also be released if we take m sufficiently large. We have a similar result for $p = 2$ with $m \geq 5$ (see Theorem 3.3.1 in Chapter 3).

Theorem 1.0.1. *Let p be an odd prime, $\chi_1, \ldots, \chi_s$ be mod p^m characters with at least one of them primitive. Suppose that $m \geq 2$ and (1.6) holds. If the $\chi_i = (\chi_i')^{k_i}$ for some primitive characters χ_i' mod p^m such that $\chi_1' \ldots \chi_s'$ is a primitive mod p^m character, and for all i, the $A_i^{-1}Bc_i'v'^{-1} \equiv \alpha_i^{k_i}$ mod p^m for some α_i, where for a primitive root a, the c_i' are defined by*

$$\chi_i'(a) = e_{\phi(p^m)}(c_i'), \quad v' := c_1' + \cdots + c_s',$$

then

$$|\mathcal{J}_1| = (k_1, p-1)\cdots(k_s, p-1)p^{\frac{m}{2}(s-1)}.$$

Otherwise $\mathcal{J}_1 = 0$.

The following evaluation of $\mathcal{J}_2$ is a special case of Theorem 4.0.1 which we shall prove in Chapter 4. Again we have stated the theorem here for $|\mathcal{J}_2|$, but in Theorem 4.0.1 in Chapter 4 we obtain an evaluation for $\mathcal{J}_2$ without assuming that condition (1.8) holds. The corresponding $p = 2$ result is given in Theorem 4.0.1 for $\mathcal{J}_2$.

Theorem 1.0.2. *Let p be an odd prime and $\chi, \chi_1, \ldots, \chi_s$ be mod p^m characters with χ primitive. Suppose that $m \geq 2$ and (1.8) holds. Let $k := 1 - \sum_{i=1}^{s} w_i$, where w_i are arbitrary integers. If $\chi\chi_1\cdots\chi_s = \chi_*^k$ for some primitive mod p^m character χ_* such that the $\chi_i\chi_*^{w_i}$ are all primitive characters mod p^m, and λ defined as:*

$$\lambda := -B\prod_{i=1}^{s}\left(c_i c_*^{-1} + w_i\right)^{w_i} \mod p^m$$

is a kth power mod p^m, then

$$|\mathcal{J}_2| = (k, p-1)p^{\frac{ms}{2}}$$

where for a primitive root a, c_i and c_* are defined as

$$\chi_i(a) = e_{\phi(p^m)}(c_i), \quad \chi_*(a) = e_{\phi(p^{m-n})}(c_*).$$

Otherwise $\mathcal{J}_2 = 0$.

Both sums $\mathcal{J}_1$ and $\mathcal{J}_2$ can be expressed in terms of the classical Gauss sums (1.3), see Theorem 3.1.1 in Chapter 3 and Theorem 4.2.1 in Chapter 4. We could have used the Gauss sum evaluations or the Cochrane and Zheng technique directly to evaluate our sums $\mathcal{J}_1$ and $\mathcal{J}_2$, but we will use the evaluation of the Jacobi sums from [15].

It would be nice if in the future one could determine which classes of exponential or character sums possess an explicit representation in terms of Gauss sums.

Chapter 2

Preliminaries

We shall start this chapter by introducing Dirichlet characters which will later be used to define Gauss and Jacobi sums.

2.1 Dirichlet Characters

Characters

Let G be a finite abelian group. A character χ on G is a non-zero function from G to $\mathbb{C}$ with $\chi(ab) = \chi(a)\chi(b)$ for all a, $b \in G$. If we denote the identity element of G as e, then for any $a \in G$ we clearly have $\chi(a) = \chi(ae) = \chi(a)\chi(e)$. Since χ is a non-zero function, we must have $\chi(e) = 1$ and so, since $a^{|G|} = e$, we get $\chi(a)^{|G|} = \chi(e) = 1$. Thus $\chi(a)$ is a $|G|$-th root of unity. The set of such characters will be denoted by $\widehat{G}$. Note $\widehat{G}$ form a group. For any two characters χ_1, χ_2 in $\widehat{G}$, we have that $\chi_1\chi_2(a) := \chi_1(a)\chi_2(a)$ is also a character where $a \in G$. The character which send every element to 1 acts as identity under multiplication and is denoted as χ_0, the principal character. The inverse of a character χ is its complex conjugate defined by $\chi^{-1}(x) = \overline{\chi(x)}$. If $\chi \in \widehat{G}$, then $\chi^{-1} \in \widehat{G}$. $\widehat{G}$ is an abelian group since multiplication in $\mathbb{C}^*$ is commutative. Note $G \cong \mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_k}$ so G is generated by elements $a_1, \ldots, a_k$ of order $n_1, \ldots, n_k$, respectively. Therefore χ is defined by

$\chi(a_j)$ where the $\chi(a_j)$ are n_jth roots of unity. Thus we have n_j choices for $\chi(a_j)$ and have $n_1 \cdots n_k$ choices for χ. So $|\widehat{G}| = n_1 \cdots n_k = |G|$. In fact, it is easy to see that $\widehat{G}$ is generated by $\chi_1, \ldots, \chi_k$ where $\chi_l(a_l) = e^{2\pi i/n_l}$ and $\chi_l(a_j) = 1$ for all $j \neq l$ so that $G \cong \widehat{G}$. In this thesis we interested in the case $G = \mathbb{Z}_q^*$. Here we use $\mathbb{Z}_q$ for $\mathbb{Z}/q\mathbb{Z}$, the ring of integers mod q and $\mathbb{Z}_q^* = \{a \in \mathbb{Z}_q : (a, q) = 1\}$, the multiplicative group of units in $\mathbb{Z}_q$. There are $\phi(q)$ distinct Dirichlet characters modulo q, where $\phi(q)$ is the Euler totient function. The $\phi(q)$ characters on $\mathbb{Z}_q^*$ can be extended to multiplicative functions on all of $\mathbb{Z}_q$ by setting $\chi(x) = 0$ when $x \notin \mathbb{Z}_q^*$.

Dirichlet Characters

For a positive integer q, we can think of a Dirichlet character mod q as a not identically zero function $\chi : \mathbb{Z} \mapsto \mathbb{C}$ with

(1) $\chi(a) = 0$ if $(a, q) > 1$,

(2) χ is completely multiplicative, that is $\chi(ab) = \chi(a)\chi(b)$ for all $a, b \in \mathbb{Z}$,

(3) χ is periodic with period q, that is $\chi(a + q) = \chi(a)$ for all $a \in \mathbb{Z}$.

More elementary properties of characters can be found in [[3], Chapter 6] and [[9], pp.88-91].

Principal Character

The principal Dirichlet character $\chi_0 \pmod{q}$ is the character with

$$\chi_0(a) := \begin{cases} 1, & \text{if } (a, q) = 1, \\ 0, & \text{else.} \end{cases} \tag{2.1}$$

Example

When $q = 1$ or $q = 2$, then $\phi(q) = 1$ and the principal character χ_0 is the only Dirichlet character. For $q \geq 3$, then $\phi(q) \geq 2$ so there are at least two Dirichlet characters. The following tables display all the Dirichlet characters for $q = 3, 4$ and 5.

Table 2.1: $q = 3, \phi(q) = 2$

n	1	2	3
$\chi_1(n)$	1	1	0
$\chi_2(n)$	1	-1	0

Table 2.2: $q = 4, \phi(q) = 2$

n	1	2	3	4
$\chi_1(n)$	1	0	1	0
$\chi_2(n)$	1	0	-1	0

Table 2.3: $q = 5, \phi(q) = 4$

n	1	2	3	4	5
$\chi_1(n)$	1	1	1	1	0
$\chi_2(n)$	1	-1	-1	1	0
$\chi_3(n)$	1	i	$-i$	-1	0
$\chi_4(n)$	1	$-i$	i	-1	0

We shall now introduce the Legendre symbol, which is an example of a Dirichlet character, but we need to know the following definition first to define the Legendre symbol.

Quadratic Residue

Let a and q be two integers with $(a, q) = 1$. Then a is called a quadratic residue mod q if the congruence $x^2 \equiv a \pmod{q}$ has a solution. Otherwise a is called a quadratic nonresidue mod q.

Legendre Symbol

Let $a, b \in \mathbb{Z}$, and p be an odd rational prime. Then

$$\left(\frac{a}{p}\right) := \begin{cases} 1, & \text{if } a \text{ is a quadratic residue mod p,} \\ -1, & \text{if } a \text{ is a quadratic nonresidue mod p,} \\ 0, & \text{if } p \text{ divides } a. \end{cases} \tag{2.2}$$

There are a number of useful properties of the Legendre symbol. We would like to state some of the properties in the following theorem.

Theorem 2.1.1. *Let p be an odd prime, then*

(1) $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$.

(2) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

(3) If $a \equiv b \pmod{p}$, *then* $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

(4) If $(a,p) = 1$, *then* $\left(\frac{a^2}{p}\right) = 1$ *and* $\left(\frac{a^2 b}{p}\right) = \left(\frac{b}{p}\right)$.

(5) $\left(\frac{1}{p}\right) = 1$ *and* $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = \begin{cases} 1, & \text{if } p \equiv 1 \mod 4, \\ -1, & \text{if } p \equiv 3 \mod 4. \end{cases}$

(6) $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = \begin{cases} 1, & \text{if } p \equiv 1 \text{ or } 7 \mod 8, \\ -1, & \text{if } p \equiv 3 \text{ or } 5 \mod 8. \end{cases}$

(7) Gaussian reciprocity law: If p and q are distinct odd primes, then

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)}{2}\cdot\frac{(q-1)}{2}}.$$

The proof of all the above properties can be found in [13, Chapter 3].

Induced Modulus

Let χ be a Dirichlet character mod q. For $q_1 \mid q$ we say that χ is an induced by a mod q_1 character, χ_{q_1}, if

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

Equivalently, q_1 is called an induced modulus for χ if we have

$$\chi(a) = 1 \text{ whenever } (a,q) = 1 \text{ and } a \equiv 1 \bmod q_1.$$

Note that for any Dirichlet character χ mod q the modulus q itself is always an induced modulus.

Primitive Characters

A Dirichlet character mod q is said to be primitive if it has no induced modulus $d < q$. A principal character χ_0 mod q is an example of a nonprimitive character for any $q \geq 2$ since it has $q_1 = 1$ as an induced modulus. If χ is a nonprincipal character mod p, where p is a prime, then χ is a primitive character mod p (since 1 cannot be an induced modulus, which is the only proper divisor of p). Thus, every nonprincipal character χ mod a prime p is a primitive character mod p.

Primitive Root

An integer a is called a primitive root mod q if $\phi(q)$ is the smallest positive integer such that $a^{\phi(q)} \equiv 1 \bmod q$. In this thesis we are concerned with the case where χ has prime power modulus, $q = p^m$ where p is a prime. A primitive root always exists when $q = p^m$ is a power of an odd prime, see [3, Chapter 10]. Let $q = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ where $p_1, p_2, \ldots, p_k$ are distinct primes and $\alpha_1, \alpha_2, \ldots, \alpha_k$ are positive integers. Suppose we have the characters $\chi_1(\bmod p_1^{\alpha_1}), \chi_2(\bmod p_2^{\alpha_2}), \ldots, \chi_k(\bmod p_1^{\alpha_k})$. Then, we can construct a mod q character χ with

$$\chi := \chi_1 \chi_2 \cdots \chi_k. \tag{2.3}$$

We claim that if $\chi_i \neq \chi_i^{'}$ for some i, then $\chi := \chi_1 \chi_2 \cdots \chi_k \neq \chi_1^{'} \chi_2^{'} \cdots \chi_k^{'} =: \chi^{'}$. Without loss of generality, suppose $\chi_1 \neq \chi_1^{'}$, then there exists an a with $(a, p_1^{\alpha_1}) = 1$ such that $\chi_1(a) \neq \chi_1^{'}(a)$. If we take m such that $m \equiv a \mod p_1^{\alpha_1}$ and $m \equiv 1 \mod p_i^{\alpha_i}$ for all $i = 2, 3, \ldots, k$, then

$$\chi(m) = \chi_1(a)\chi_2(1) \cdots \chi_k(1) = \chi_1(a), \text{ and } \chi^{'}(m) = \chi_1^{'}(a)\chi_2^{'}(1) \cdots \chi_k^{'}(1) = \chi_1^{'}(a).$$

Since $\chi_1(a) \neq \chi_1'(a)$ we get $\chi(m) \neq \chi'(m)$ and so $\chi \neq \chi^{'}$. Furthermore, there are $\phi(p_i^{\alpha_i})$ characters mod $p_i^{\alpha_i}$ for all $i = 1, 2, \ldots, k$, so we can make $\phi(p_1^{\alpha_1})\phi(p_2^{\alpha_2}) \cdots \phi(p_k^{\alpha_k}) = \phi(q)$ distinct characters mod q. Consequently, every mod q character can be written as the product

k mod q characters induced by mod $p_i^{\alpha_i}$ characters, $i = 1, 2, \ldots, k$. Note that the value of φ on prime powers p^α is

$$\phi(p^\alpha) = p^{\alpha-1}(p-1).$$

Additionally, χ is a primitive character if and only if $\chi_1, \chi_2, \ldots, \chi_k$ are primitive characters.

Lemma 2.1.1. *Let χ be a Dirichlet character mod q. Then,*

$$\sum_{a \bmod q} \chi(a) = \begin{cases} \phi(q), & \text{if } \chi = \chi_0 \ , \\ 0, & \text{otherwise.} \end{cases} \tag{2.4}$$

Proof. Let

$$S := \sum_{a \bmod q} \chi(a).$$

Let c be any integer with $(c, q) = 1$. Then,

$$\chi(c)S = \sum_{a \bmod q} \chi(c)\chi(a) = \sum_{a \bmod q} \chi(ca).$$

Define $b := ca$. Since a ranges over all the residue classes mod q, so does b. Therefore,

$$\chi(c)S = \sum_{b \bmod q} \chi(b) = S.$$

Thus, either $S = 0$ or $\chi(c) = 1$. Since c was an arbitrary reduced residue class mod q, we must have either $S = 0$ or $\chi(c) = 1$ for all reduced residue classes mod q. In other word, either $S = 0$ or $\chi = \chi_0$. When $\chi = \chi_0$ we have

$$S = \sum_{a \bmod q} \chi_0(a) = \phi(q).$$

□

Let $\vec{f} := (f_1, \ldots, f_k)$ where $f_i \in \mathbb{Z}[x_1, \ldots, x_s]$ for all $i = 1, \ldots, k$. Let $\vec{\chi} = (\chi_1, \ldots, \chi_k)$ denote k characters χ_i mod q, then for $g \in \mathbb{Z}[x_1, \ldots, x_s]$, define the more general sum

$$S(\vec{\chi}, \vec{f}, q) := \sum_{\substack{x_1=1 \\ g(x_1,\ldots,x_s)\equiv 0 \bmod q}}^{q} \cdots \sum_{x_s=1}^{q} \chi_1(f_1(x_1, \ldots, x_s)) \cdots \chi_k(f_k(x_1, \ldots, x_s)). \tag{2.5}$$

When q is composite the following lemma can be used to reduce sums of the form (2.5) to the case of prime power modulus.

Lemma 2.1.2. *Suppose that $\chi_1, \ldots, \chi_k$ are mod uv characters with $(u, v) = 1$. Writing $\chi_i = \chi_i' \chi_i''$ for mod u and mod v characters χ_i' and χ_i'' respectively, where $i = 1, \ldots, k$, then*

$$S(\vec{\chi}, \vec{f}, uv) = S(\vec{\chi'}, \vec{f}, u) S(\vec{\chi''}, \vec{f}, v).$$

Proof. For all $i = 1, \ldots, k$, suppose that χ_i is a mod uv character with $(u, v) = 1$, and $\chi_i = \chi_i' \chi_i''$, where χ_i' is a mod u and χ_i'' is a mod v character. Write $x_i = e_i v v^{-1} + t_i u u^{-1}$, where $uu^{-1} + vv^{-1} = 1$ and $e_i = 1, \ldots, u$, $t_i = 1, \ldots, v$. Note

$$\begin{aligned}\chi_i(f_i(x_1, \ldots, x_s)) &= \chi_i' \chi_i''(f_i(e_1 v v^{-1} + t_1 u u^{-1}, \ldots, e_s v v^{-1} + t_s u u^{-1})) \\ &= \chi_i'(f_i(e_1, \ldots, e_s)) \chi_i''(f_i(t_1, \ldots, t_s)).\end{aligned}$$

Since $(u, v) = 1$, we have

$$g(x_1, \ldots, x_s) \equiv 0 \bmod uv \Leftrightarrow \begin{cases} g(x_1, \ldots, x_s) \equiv 0 \bmod u, \\ g(x_1, \ldots, x_s) \equiv 0 \bmod v, \end{cases} \Leftrightarrow \begin{cases} g(e_1, \ldots, e_s) \equiv 0 \bmod u, \\ g(t_1, \ldots, t_s) \equiv 0 \bmod v. \end{cases}$$

Writing $S := S(\vec{\chi}, \vec{f}, uv)$, then we have

$$S = \sum_{\substack{e_1=1 \\ g(e_1,\ldots,e_s)\equiv 0 \bmod u \\ g(t_1,\ldots,t_s)\equiv 0 \bmod v}}^{u} \sum_{t_1=1}^{v} \cdots \sum_{e_s=1}^{u} \sum_{t_s=1}^{v} \chi_1'(f_1(e_1,\ldots,e_s))\chi_1''(f_1(t_1,\ldots,t_s)) \cdots \chi_k'(f_k(e_1,\ldots,e_s))\chi_k''(f_k(t_1,\ldots,t_s))$$

$$= \sum_{\substack{e_1=1 \\ g(e_1,\ldots,e_s)\equiv 0 \bmod u}}^{u} \cdots \sum_{e_s=1}^{u} \chi_1'(f_1(e_1,\ldots,e_s)) \cdots \chi_k'(f_k(e_1,\ldots,e_s))$$

$$\times \sum_{\substack{t_1=1 \\ g(t_1,\ldots,t_s)\equiv 0 \bmod v}}^{v} \cdots \sum_{t_s=1}^{v} \chi_1''(f_1(t_1,\ldots,t_s)) \cdots \chi_k''(f_k(t_1,\ldots,t_s))$$

$$= S(\vec{\chi'}, \vec{f}, u)S(\vec{\chi''}, \vec{f}, v).$$

□

Since the sums in (1.5) and (1.7) are special case of (2.5), we can reduce them to the case of prime power.

2.2 Gauss Sums

For a mod q Dirichlet character χ we define the Gauss sum by

$$G(\chi, q) := \sum_{x=1}^{q} \chi(x)e_q(x), \tag{2.6}$$

where we recall that $e_k(x) = e^{2\pi ix/k}$. In view of Lemma 2.1.2 we restrict ourself to the case when q is a prime power, p^m. When $q = p$ and χ is the Legendre symbol, $G(\chi, p)$ is called a quadratic Gauss sum, and will be denoted simply as $\mathcal{G}_p$. We would like to start with the following Lemma in order to understand the Gauss sums properties.

Lemma 2.2.1.

$$\sum_{x=0}^{q-1} e_q(Ax) = \begin{cases} q, & \textit{if } A \equiv 0 \ \textit{mod } q, \\ 0, & \textit{else.} \end{cases} \tag{2.7}$$

Proof. If $A \equiv 0$ mod q, then $e_q(Ax) = 1$, and $\sum_{x=0}^{q-1} e_q(Ax) = \sum_{x=0}^{q-1} 1 = q$. If $A \not\equiv 0$ mod q, then $e_q(A) \neq 1$ and

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

□

More generally we can define

$$\mathfrak{S}(A, \chi) := \sum_{x=1}^{q} \chi(x) e_q(Ax). \tag{2.8}$$

If $A = 1$, then $\mathfrak{S}(1, \chi) = G(\chi, q)$.

Theorem 2.2.1. *If χ is a primitive character mod q, then $\mathfrak{S}(A, \chi) = 0$ for all $(A, q) \neq 1$.*

Proof. Suppose $\mathfrak{S}(A, \chi) \neq 0$ for some $(A, q) > 1$, then we need to show χ is imprimitive. Take $q_1 := q/(A, q)$ and suppose that $m \equiv 1$ mod q_1 with $(m, q) = 1$. Note

$$\begin{aligned} e_q(Ajm) &= e^{\frac{2\pi i Ajm}{q}} = e^{\frac{2\pi i Ajm}{q_1 (A,q)}} \\ &= e_{q_1}\left(\frac{Aj}{(A, q)} m\right)) = e_{q_1}\left(\frac{Aj}{(A, q)}\right) \\ &= e^{\frac{2\pi i Aj}{q_1 (A,q)}} = e^{\frac{2\pi i Aj}{q}} \\ &= e_q(Aj). \end{aligned}$$

Thus we have

$$\begin{aligned}\mathfrak{S}(A,\chi) &= \sum_{j \bmod q} \chi(j)e_q(Aj) \\ &= \sum_{j \bmod q} \chi(jm)e_q(Ajm) \quad j := jm \\ &= \chi(m)\sum_{j=1}^{q} \chi(j)e_q(Aj) \\ &= \chi(m)\mathfrak{S}(A,\chi).\end{aligned}$$

Since $\mathfrak{S}(A,\chi) \neq 0$ we must have $\chi(m) = 1$ which shows that χ is induced by a mod q_1 character. Thus χ is imprimitive.

□

Proposition 2.2.1. *If χ is any Dirichlet character mod q, then*

$$\mathfrak{S}(A,\chi) = \overline{\chi(A)}\mathfrak{S}(1,\chi) \quad \textit{whenever } (A,q) = 1.$$

Proof. Let $\mathfrak{S}(A,\chi) = \sum_{x=1}^{q} \chi(x)e_q(Ax)$. When $(A,q) = 1$, the numbers Ax run through a complete residue system mod q with x. Also, $|\chi(A)|^2 = \chi(A)\overline{\chi(A)} = 1$ so

$$\chi(x) = \overline{\chi(A)}\chi(A)\chi(x) = \overline{\chi(A)}\chi(Ax).$$

Therefore the sum defining $\mathfrak{S}(A,\chi)$ can be written as follows:

$$\begin{aligned}\mathfrak{S}(A,\chi) &= \sum_{x=1}^{q}\chi(x)e_q(Ax)\\ &= \overline{\chi(A)}\sum_{x=1}^{q}\chi(Ax)e_q(Ax)\\ &= \overline{\chi(A)}\sum_{y=1}^{q}\chi(y)e_q(y), \quad y := Ax\\ &= \overline{\chi(A)}\mathfrak{S}(1,\chi).\end{aligned}$$

□

Corollary 2.2.1. *Assume $q = p$ and $\chi = \left(\frac{x}{p}\right)$, the Legendre symbol, then*

$$\mathfrak{S}(A,\chi) = \left(\frac{A}{p}\right)\mathfrak{S}(1,\chi).$$

Proposition 2.2.2. *If χ is a primitive character mod q, then*

$$|\mathfrak{S}(A,\chi)| = \begin{cases}\sqrt{q}, & \text{if } (A,q) = 1,\\ 0, & \text{if } (A,q) \neq 1.\end{cases}$$

Proof. Suppose χ is a primitive character mod q. From Theorem 2.2.1 we know that $\mathfrak{S}(A,\chi) = 0$ whenever $(A,q) \neq 1$. Now suppose $(A,q) = 1$. If $A \neq 0$, then by Proposition 2.2.1 we have $\mathfrak{S}(A,\chi) = \overline{\chi(A)}\mathfrak{S}(1,\chi)$, and so

$$\begin{aligned}|\mathfrak{S}(A,\chi)|^2 &= \mathfrak{S}(A,\chi)\overline{\mathfrak{S}(A,\chi)}\\ &= \left(\overline{\chi(A)}\mathfrak{S}(1,\chi)\right)\left(\chi(A)\overline{\mathfrak{S}(1,\chi)}\right)\\ &= |\mathfrak{S}(1,\chi)|^2.\end{aligned}$$

Furthermore

$$
\begin{aligned}
|\mathfrak{S}(1,\chi)|^2 &= \sum_{j \bmod q} \chi(j)e_q(j) \sum_{k \bmod q} \overline{\chi(k)}e_q(-k) \\
&= \sum_{(k,q)=1} \overline{\chi(k)} \left(\sum_j \chi(j)e_q(j) \right) e_q(-k) \\
&= \sum_{(k,q)=1} \overline{\chi(k)} \left(\sum_j \chi(jk)e_q(jk) \right) e_q(-k), \quad j := jk \\
&= \sum_{(k,q)=1} e_q(-k) \left(\sum_j \chi(j)e_q(jk) \right).
\end{aligned}
$$

By Theorem 2.2.1 the sum $\sum_j \chi(j)e_q(jk) = 0$ if $(k,q) \neq 1$ thus

$$
\begin{aligned}
|\mathfrak{S}(1,\chi)|^2 &= \sum_{k=1}^{q} \sum_{j=1}^{q} \chi(j)e_q(k(j-1)) \\
&= \sum_{j=1}^{q} \chi(j) \left(\sum_{k=1}^{q} e_q(k(j-1)) \right).
\end{aligned}
$$

Since

$$
\sum_{k=1}^{q} e_q(k(j-1)) = \begin{cases} q, & \text{if } j-1 \equiv 0 \pmod q, \\ 0, & \text{if } j-1 \not\equiv 0 \pmod q, \end{cases}
$$

we have $|\mathfrak{S}(1,\chi)|^2 = q\chi(1) = q$.

□

The following lemma plays a useful role for proofing the main sums in this thesis (1.5) in Chapter 3 and (1.7) in Chapter 4 (which can be seen in [16]).

Lemma 2.2.2. *For any u with $(u,p)=1$, if u is a kth power mod p^m, then*

$$\sum_{\chi^k=\chi_0 \bmod p^m} \chi(u) = D := \begin{cases} (k,\phi(p^m)), & \text{if } p \text{ is odd or } p^m = 2,4, \\ 2(k,2^{m-2}), & \text{if } p=2,\ m\geq 3,\ k \text{ is even}, \\ 1, & \text{if } p=2,\ m\geq 3,\ k \text{ is odd.} \end{cases} \tag{2.9}$$

If u is not a kth power mod p^m, then

$$\sum_{\chi^k=\chi_0 \bmod p^m} \chi(u) = 0.$$

Proof. We know that there are exactly $\phi(p^m)$ characters mod p^m. We claim that D of these characters have the property $\chi^k = \chi_0$. For p is odd, we have a primitive root a mod p^m and define the character χ as

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

If $\chi^k = \chi_0$, then we have

$$e_{\phi(p^m)}(c) = \chi(a)^k = \chi_0(a) = e_{\phi(p^m)}(0).$$

Thus we have the congruence $ck \equiv 0 \mod \phi(p^m)$. Let $D = (k, \phi(p^m))$. Then $c \equiv 0 \mod \phi(p^m)/D$ so $c = \phi(p^m)j/D$ where $j = 1, \ldots, (k, \phi(p^m))$. Therefore there are exactly D characters such that

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

Thus if u is a kth power mod p^m, then

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

If u is not a kth power mod p^m, then $u = a^\gamma$ where $\gamma \not\equiv k\gamma'$ mod $\phi(p^m)$ for some γ' and so $D \nmid \gamma$, and by using (2.7) we get

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

For $p = 2$, $m \geq 3$. We need two generators $a = -1$ and $a = 5$ for $\mathbb{Z}^*_{2^m}$ (see [13]). Define

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

If $\chi^k = \chi_0$, then we have the congruences $kc \equiv 0 \bmod 2^{m-2}$ and $kc_0 \equiv 0 \bmod 2$ which have $(k, 2^{m-2})$ and $(k, 2)$ solutions, respectively. Therefore if k even, there are exactly $D = 2(k, 2^{m-2})$ characters such that $\chi^k = \chi_0$. If $(k, 2) = 1$, then $D = 1$ and there is only the principal character with $\chi^k = \chi_0$. Thus, if u is a kth power mod 2^m, then

$$\sum_{\chi^k=\chi_0 \bmod p^m} \chi(u) = \begin{cases} 2(k, 2^{m-2}), & \text{if } p = 2,\ m \geq 3,\ k \text{ even}, \\ 1, & \text{if } p = 2,\ m \geq 3,\ k \text{ odd}. \end{cases}$$

If k is odd then every odd u is a kth power. If u is not a kth power mod 2^m and k even, then $u = (-1)^\gamma(5)^\beta$ where $2 \nmid \gamma$ or $(k, 2^{m-2}) \nmid \beta$. Therefore by using again (2.7) we get

$$\sum_{\chi^D=\chi_0} \chi(u) = \sum_{\chi^D=\chi_0} \chi(-1)^\gamma \chi(5)^\beta = \sum_{x=1}^{2} e_2(x\gamma) \sum_{y=1}^{D} e\left(\frac{y\beta}{(k, 2^{m-2})}\right).$$

Therefore, if $2 \nmid \gamma$ then the sum $\sum_{x=1}^{2} e_2(x\gamma) = 0$ or if $(k, 2^{m-2}) \nmid \beta$. then the sum $\sum_{y=1}^{D} e\left(\frac{y\beta}{(k,2^{m-2})}\right) = 0$. Thus

$$\sum_{\chi^D=\chi_0} \chi(u) = 0.$$

Note, if $p = 2$, and $m = 1$, then $\phi(2) = 1$ which shows that we have only one character, the principal character χ_0 and $u^k \equiv u \bmod 2$

$$\chi^k(u) = \chi_0(u) = 1.$$

If $p = 4$, then as seen in Table 2.2 we have two characters χ_1, χ_2 where

$$\chi_1(u) = \begin{cases} 0, & \text{if } u \text{ is even,} \\ 1, & \text{if } u \text{ is odd,} \end{cases} \quad \text{and} \quad \chi_2(u) = \begin{cases} 1, & \text{if } u \equiv 1 \bmod 4, \\ -1, & \text{if } u \equiv 3 \bmod 4, \\ 0, & \text{if } u \equiv 0 \bmod 4. \end{cases}$$

Thus, we get

$$\sum_{\chi^k = \chi_0} \chi(u) = \begin{cases} 0, & \text{if } k \text{ even and } u \equiv 3 \bmod 4, \\ 2, & \text{if } k \text{ is even and } u \equiv 1 \bmod 4, \\ 1, & \text{if } k \text{ is odd.} \end{cases}$$

□

Recall that $\mathcal{G}_p$ is the quadratic Gauss sum,

$$\mathcal{G}_p := \sum_{x=1}^{p-1} \left(\frac{x}{p}\right) e_p(x). \tag{2.10}$$

where $\left(\frac{x}{p}\right)$ is the Legendre symbol.

Lemma 2.2.3. *For any odd prime p we have $\mathcal{G}_p^2 = \left(\frac{-1}{p}\right) p$. Moreover,*

$$\mathcal{G}_p := \sum_{x=0}^{p-1} e_p(x^2) = \begin{cases} \pm\sqrt{p}, & \text{if } p \equiv 1 \bmod 4, \\ \pm i\sqrt{p}, & \text{if } p \equiv 3 \bmod 4. \end{cases} \tag{2.11}$$

Proof. Determining the sign is a more difficult problem and will not be done here. In fact, Gauss proved the remarkable formula (see Theorem 1.3.4 in [4]),

$$\mathcal{G}_p = \begin{cases} \sqrt{p}, & \text{if } p \equiv 1 \bmod 4, \\ i\sqrt{p}, & \text{if } p \equiv 3 \bmod 4. \end{cases}$$

From the definition of the quadratic Gauss sum, we have

$$\begin{aligned} \mathcal{G}_p^2 &= \sum_{x=1}^{p-1} \left(\frac{x}{p}\right) e_p(x) \sum_{y=1}^{p-1} \left(\frac{y}{p}\right) e_p(y) \\ &= \sum_{x=1}^{p-1} \left(\frac{x}{p}\right) e_p(x) \left(\sum_{y=1}^{p-1} \left(\frac{xy}{p}\right) e_p(xy) \right) \\ &= \sum_{y=1}^{p-1} \left(\frac{y}{p}\right) \sum_{x=1}^{p-1} e_p(x(y+1)). \end{aligned}$$

Now for $y = 1, \ldots, p-2$, $x(y+1)$ runs through a reduced residue system mod p as x goes from 1 to $p-1$ and so $\sum_{x=1}^{p-1} e_p(x(y+1)) = \sum_{x=1}^{p-1} e_p(x) = -1$. For $y = p-1$ the sum over x is just a sum of 1's. Thus we get

$$\begin{aligned} \mathcal{G}_p^2 &= (-1) \sum_{y=1}^{p-2} \left(\frac{y}{p}\right) + \left(\frac{-1}{p}\right)(p-1) \\ &= (-1) \sum_{y=1}^{p-1} \left(\frac{y}{p}\right) + \left(\frac{-1}{p}\right) + \left(\frac{-1}{p}\right)(p-1) = \left(\frac{-1}{p}\right) p. \end{aligned}$$

From the property (5) in Lemma 2.1.1 we get the desired result.

□

2.3 Jacobi Sums

Definition 2.3.1. *For two Dirichlet characters χ_1, χ_2 mod q, we define the classical Jacobi sums as*

$$J(\chi_1, \chi_2, q) := \sum_{x=1}^{q} \chi_1(x)\chi_2(1-x). \tag{2.12}$$

Recall that a nonprincipal character is the same as a primitive character on $\mathbb{Z}_p$, when p is a prime.

Theorem 2.3.1. *Let χ_1 and χ_2 be characters on $\mathbb{Z}_p$, where p is a prime.*
(a) If χ_1 and χ_2 are both principal characters, then $J(\chi_1, \chi_2, p) = p - 2$.
(b) If one of χ_1 and χ_2 is principal, then $J(\chi_1, \chi_2, p) = -1$.
(c) If χ is nonprincipal, then $J(\overline{\chi}, \chi, p) = -\chi(-1)$.

Proof. (a) Since both χ_1 and χ_2 are principal, we have

$$J(\chi_1, \chi_2, p) = \sum_{x \in \mathbb{Z}_p} \chi_1(x)\chi_2(1-x) = \sum_{x \neq 0,1} \chi_1(x)\chi_2(1-x) = p - 2.$$

(b) Suppose χ_1 is principal and χ_2 is nonprincipal. Then we have $\chi_1(x) = 1$ for $x \neq 0$ and

$$J(\chi_1, \chi_2, p) = \sum_{x \in \mathbb{Z}_p^*} \chi_2(1-x) = \sum_{x \in \mathbb{Z}_p} \chi_2(1-x) - \chi_2(1) = 0 - \chi_2(1) = -1.$$

(c) If χ is nonprincipal, then

$$\begin{aligned} J(\overline{\chi}, \chi, p) &= \sum_{x \in \mathbb{Z}_p^*} \chi(x^{-1})\chi(1-x) = \sum_{x \in \mathbb{Z}_p^*} \chi(x^{-1} - 1) \\ &= \sum_{x \in \mathbb{Z}_p^*} \chi(x-1) = \sum_{x \in \mathbb{Z}_p} \chi(x-1) - \chi(-1) = -\chi(-1). \end{aligned}$$

□

The following theorem shows that the mod q Jacobi sums (2.12) can be written in terms of Gauss sums (as in Theorem 2.1.3 of [4] or Theorem 5.21 of [11]).

Lemma 2.3.1. *If* χ_1, χ_2 *are characters mod* q *such that* $\chi_1\chi_2$ *is primitive, then for any* $z \in \mathbb{Z}$

$$\sum\sum_{x_1+x_2\equiv z \bmod q} \chi_1(x_1)\chi_2(x_2) = \chi_1\chi_2(z)J(\chi_1, \chi_2, q).$$

Note, if $(z, q) \neq 1$*, and* $\chi_1\chi_2$ *is primitive character mod* q*, then the above sum will be zero.*

Proof. Suppose χ_1, χ_2 are characters mod q with $(z, q) = 1$, then from the change of variable $x_1 \mapsto x_1 z$ and $x_2 \mapsto x_2 z$ we get

$$\begin{aligned}\sum\sum_{x_1+x_2\equiv z \bmod q} \chi_1(x_1)\chi_2(x_2) &= \chi_1\chi_2(z) \sum\sum_{x_1+x_2\equiv 1 \bmod q} \chi_1(x_1)\chi_2(x_2) \\ &= \chi_1\chi_2(z)J(\chi_1, \chi_2, q).\end{aligned}$$

If $(z, q) \neq 1$, and $\chi_1\chi_2$ is primitive, then there is a $u \equiv 1 \mod q/(z, q)$ with $\chi_1\chi_2(u) \neq 1$ and $(u, q) = 1$. Thus, the change of variable $x_i \mapsto x_i u$, $i = 1, 2$ with the observation that $z \equiv zu$ mod q give that

$$\sum\sum_{x_1+x_2\equiv z \bmod q} \chi_1(x_1)\chi_2(x_2) = \chi_1\chi_2(u) \sum\sum_{x_1+x_2\equiv z \bmod q} \chi_1(x_1)\chi_2(x_2).$$

Hence

$$\sum\sum_{x_1+x_2\equiv z \bmod q} \chi_1(x_1)\chi_2(x_2) = 0.$$

□

Theorem 2.3.2. *Let* χ_1 *and* χ_2 *be mod* q *characters. If* $\chi_1\chi_2$ *is primitive, then*

$$J(\chi_1, \chi_2, q) = \frac{G(\chi_1, q)G(\chi_2, q)}{G(\chi_1\chi_2, q)},$$

and if χ_1, χ_2, and $\chi_1\chi_2$ are all primitive, then

$$|J(\chi_1,\chi_2,q)| = q^{1/2}.$$

Proof. By the definition of Gauss sums given in (2.6) and Lemma 2.3.1 we have

$$\begin{aligned} G(\chi_1,q)G(\chi_2,q) &= \sum_x\sum_y \chi_1(x)\chi_2(y)e_q(x+y) \\ &= \sum_z e_q(z)\sum_{x+y=z}\chi_1(x)\chi_2(y) \\ &= J(\chi_1,\chi_2,q)\sum_z \chi_1\chi_2(z)e_q(z) \\ &= J(\chi_1,\chi_2,q)G(\chi_1\chi_2,q). \end{aligned}$$

Now suppose that χ_1, χ_2, and $\chi_1\chi_2$ are all primitive. Then from Proposition 2.2.2, we get

$$|J(\chi_1,\chi_2,q)| = \frac{|G(\chi_1,q)||G(\chi_2,q)|}{|G(\chi_1\chi_2,q)|} = \frac{q^{1/2}q^{1/2}}{q^{1/2}} = q^{1/2}.$$

□

2.4 Generalized Jacobi Sums

Definition 2.4.1. *Let $\chi_1,\dots,\chi_s$ be mod q characters. Then the generalized Jacobi sum $J(\chi_1,\dots,\chi_s,q)$ is defined by*

$$J(\chi_1,\dots,\chi_s,q) := \sum_{x_1+\cdots+x_s\equiv 1 \bmod q} \chi_1(x_1)\cdots\chi_s(x_s), \tag{2.13}$$

where the summation is taken over all q^{s-1} s-tuples $(x_1,\dots,x_s)$ of elements of $\mathbb{Z}_q$ with $x_1+\cdots+x_s = 1$.

When $s = 1$, the sum (2.13) is

$$J(\chi_1, q) = \chi_1(1) = 1.$$

When $s = 2$ this definition agrees with the definition given in (2.12). As usual we restrict ourselves to the case of prime powers. Let $\chi_1, \ldots, \chi_s$ be mod p^m characters and $B \in \mathbb{Z}$. Define

$$J_B(\chi_1, \ldots, \chi_s, p^m) := \sum_{\substack{x_1=1 \\ x_1+\cdots+x_s \equiv B \bmod p^m}}^{p^m} \cdots \sum_{x_s=1}^{p^m} \chi_1(x_1) \cdots \chi_s(x_s). \tag{2.14}$$

When $B = p^n B'$ where $p \nmid B'$ and $n < m$, then the simple change of variables $x_i \mapsto x_i B'$, $i = 1, \ldots, s$ gives

$$\begin{aligned} J_B(\chi_1, \ldots, \chi_s, p^m) &= \sum_{\substack{x_1=1 \\ B'(x_1+\cdots+x_s) \equiv p^n B' \bmod p^m}}^{p^m} \cdots \sum_{x_s=1}^{p^m} \chi_1(x_1 B') \cdots \chi_s(x_s B') \\ &= (\chi_1 \cdots \chi_s)(B') \sum_{\substack{x_1=1 \\ x_1+\cdots+x_s \equiv p^n \bmod p^m}}^{p^m} \cdots \sum_{x_s=1}^{p^m} \chi_1(x_1) \cdots \chi_s(x_s) \\ &= (\chi_1 \cdots \chi_s)(B') J_{p^n}(\chi_1, \ldots, \chi_s, p^m). \end{aligned} \tag{2.15}$$

For example $J_B(\chi_1, \ldots, \chi_s, p^m) = (\chi_1 \cdots \chi_s)(B) J(\chi_1, \ldots, \chi_s, p^m)$ when $p \nmid B$. The following theorem shows the case when $n \geq m$ (i.e. $B = 0$) in (2.14).

Theorem 2.4.1. *If $\chi_1, \ldots, \chi_s$ are mod p^m characters, then*

$$J_0(\chi_1, \ldots, \chi_s, p^m) = \begin{cases} \phi(p^m)\chi_s(-1) J(\chi_1, \ldots, \chi_{s-1}, p^m), & \text{if } \chi_1 \cdots \chi_s = \chi_0, \\ 0, & \text{if } \chi_1 \cdots \chi_s \neq \chi_0, \end{cases}$$

where χ_0 is the principal character.

Proof. In the sums below, the x_i run through complete residue systems mod p^m.

$$\begin{aligned}
J_0(\chi_1, \dots, \chi_s, p^m) &= \sum_{x_1+\cdots+x_s=0} \chi_1(x_1)\cdots\chi_s(x_s) \\
&= \sum_{x_s} \left(\sum_{x_1+\cdots+x_{s-1}=-x_s} \chi_1(x_1)\cdots\chi_{s-1}(x_{s-1}) \right) \chi_s(x_s) \\
&= \sum_{(x_s,p)=1} \left(\sum_{x_1+\cdots+x_{s-1}=-x_s} \chi_1(x_1)\cdots\chi_{s-1}(x_{s-1}) \right) \chi_s(x_s) \\
&= \sum_{(x_s,p)=1} \left((\chi_1\cdots\chi_{s-1})(-x_s) J(\chi_1, \dots, \chi_{s-1}, p^m)\right) \chi_s(x_s), \quad x_i \mapsto -x_i x_s \\
&= \chi_s(-1) J(\chi_1, \dots, \chi_{s-1}, p^m) \sum_{x_s} (\chi_1\cdots\chi_s)(-x_s) \\
&= \chi_s(-1) J(\chi_1, \dots, \chi_{s-1}, p^m) \sum_{x_s} (\chi_1\cdots\chi_s)(x_s).
\end{aligned}$$

Then the result follows from (2.4)

$$\sum_{x_s} \chi_1\cdots\chi_s(x_s) = \begin{cases} \phi(p^m), & \text{if } \chi_1\cdots\chi_s = \chi_0, \\ 0, & \text{if } \chi_1\cdots\chi_s \neq \chi_0. \end{cases}$$

□

Chapter 3

Evaluating Jacobi Type Sums Modulo Prime Powers

For two Dirichlet characters χ_1, χ_2 mod q the classical Jacobi sum is

$$J(\chi_1, \chi_2, q) := \sum_{x=1}^{q} \chi_1(x)\chi_2(1-x). \tag{3.1}$$

More generally, for s characters $\chi_1, \ldots, \chi_s$ mod q and an integer B, one can define a generalized Jacobi sum

$$J_B(\chi_1, \ldots, \chi_s, q) := \sum_{\substack{x_1=1 \\ x_1+\cdots+x_s \equiv B \bmod q}}^{q} \cdots \sum_{x_s=1}^{q} \chi_1(x_1) \cdots \chi_s(x_s). \tag{3.2}$$

A thorough discussion of mod p Jacobi sums and their extension to finite fields can be found in Berndt, Evans and Williams [4]. Zhang and Yao [24] showed that the sums (3.1) had an explicit evaluation when q is a perfect square and Zhang and Xu [23] obtained an evaluation of the sums (3.2) for certain classes of squareful q (if $p \mid q$, then $p^2 \mid q$) in the classic $B = 1$ case. In [15] Ostergaard, Pigno and Pinner extended this to more general squareful q and general B, essentially using reduction techniques of Cochrane and Zheng [6].

Here we are interested in an even more general sum. Let $\vec{\chi} = (\chi_1, \ldots, \chi_s)$ denote s characters χ_i mod q. Then for an $h \in \mathbb{Z}[x_1, \ldots, x_s]$ and $B \in \mathbb{Z}$ we can define

$$J_B(\vec{\chi}, h, q) := \sum_{\substack{x_1=1 \\ h(x_1,\ldots,x_s)\equiv B \bmod q}}^{q} \cdots \sum_{x_s=1}^{q} \chi_1(x_1)\cdots\chi_s(x_s). \tag{3.3}$$

As demonstrated in Lemma 2.1.2 in Chapter 2 one can usually reduce such sums to the case that $q = p^m$ is a prime power. In this chapter we will be concerned with h of the form

$$h_1 = h_1(x_1, \ldots, x_s) := A_1 x_1^{k_1} + \cdots + A_s x_s^{k_s}, \quad p \nmid A_1 \cdots A_s, \tag{3.4}$$

where the k_i are non-zero integers, and

$$\mathcal{J}_1 := J_B(\vec{\chi}, h_1, p^m) = \sum_{\substack{x_1=1 \\ A_1x_1^{k_1}+\cdots+A_sx_s^{k_s}\equiv B \bmod p^m}}^{p^m} \cdots \sum_{x_s=1}^{p^m} \chi_1(x_1)\cdots\chi_s(x_s). \tag{3.5}$$

As well as (3.2) this generalization includes the binomial character sums

$$\sum_{x=1}^{p^m} \chi_1(x)\chi_2(Ax^k + B), \tag{3.6}$$

shown to also have an explicit evaluation (see Theorem 3.1 in [18]). A different generalization of these sums having an explicit evaluation in certain special cases is considered in [22]. We define n to be the power of p dividing B

$$B = p^n B', \quad p \nmid B'. \tag{3.7}$$

The evaluation in [15] relied on expressing (3.2) in terms of Gauss sums

$$G(\chi, p^m) := \sum_{x=1}^{p^m} \chi(x) e_{p^m}(x), \tag{3.8}$$

where $e_k(x) = e^{2\pi i x/k}$. For example, if at least one of the χ_i is primitive mod p^m and $m > n$ then $J_B(\chi_1, \dots, \chi_s, p^m) = 0$ unless $\chi_1 \cdots \chi_s$ is a mod p^{m-n} character, in which case

$$J_B(\chi_1, \dots, \chi_s, p^m) = \chi_1 \cdots \chi_s(B') p^{-(m-n)} \overline{G(\chi_1 \cdots \chi_s, p^{m-n})} \prod_{i=1}^{s} G(\chi_i, p^m), \tag{3.9}$$

(see for example [15, Theorem 2.2]). In particular if $m \geq n+2$ and at least one of the χ_i is primitive we see that $J_B(\chi_1, \dots, \chi_s, p^m) = 0$ unless all the χ_i are primitive with $\chi_1 \cdots \chi_s$ primitive mod p^{m-n}. In this latter case (3.9) and a useful evaluation of the Gauss sum led in [15] to the following explicit evaluation of (3.2):

$$J_B(\chi_1, \dots, \chi_s, p^m) = p^{\frac{1}{2}(m(s-1)+n)} \frac{\chi_1(B'c_1) \cdots \chi_s(B'c_s)}{\chi_1 \cdots \chi_s(v)} \delta(\chi_1, \dots, \chi_s), \tag{3.10}$$

where, when p is odd,

$$\delta(\chi_1, \dots, \chi_s) = \left(\frac{-2r}{p}\right)^{m(s-1)+n} \left(\frac{v}{p}\right)^{m-n} \left(\frac{c_1 \cdots c_s}{p}\right)^{m} \varepsilon_{p^m}^{s} \varepsilon_{p^{m-n}}^{-1}, \tag{3.11}$$

with an extra factor $e_3(rv)$ needed when $p = m - n = 3$, $n > 0$, and for a choice of primitive root a mod p^m, the integers r and c_i are defined by

$$a^{\phi(p)} = 1 + rp, \quad \chi_i(a) = e_{\phi(p^m)}(c_i), \;\; 1 \leq c_i \leq \phi(p^m). \tag{3.12}$$

Here, as usual, $\left(\frac{x}{y}\right)$ denotes the Jacobi symbol,

$$\varepsilon_j := \begin{cases} 1, & \text{if} \quad j \equiv 1 \bmod 4, \\ i, & \text{if} \quad j \equiv 3 \bmod 4, \end{cases} \tag{3.13}$$

and

$$v := p^{-n}(c_1 + \cdots + c_s). \tag{3.14}$$

The sums (3.6) can also be expressed in terms of Gauss sums as shown in [18]. As we shall see in Theorem 3.1.1 below, our general sums (3.5) have a similar Gauss sum representation that can be used to give an explicit evaluation for sufficiently large m, though here we shall use an expression in terms of sums of type (3.2) and their evaluation (3.10). We define the parameters t_i and t by

$$p^{t_i} \mid\mid k_i, \qquad t := \max\{t_1, \ldots, t_s\}. \tag{3.15}$$

Note, it is natural to assume that $m \geq t+1$ (and $m \geq t+2$ for $p = 2$, $m \geq 3$), since if $m \leq t_i$ we have $x_i^{k_i} \equiv x_i^{k_i/p} \bmod p^m$ and one can replace k_i by k_i/p. We define d_i and D_i by

$$d_i := (k_i, p-1), \quad D_i := \begin{cases} p^{t_i} d_i, & \text{if } p \text{ is odd}, \\ 2^{t_i+1}, & \text{if } p = 2,\ k_i \text{ even}, \\ 1, & \text{if } p = 2,\ k_i \text{ odd}. \end{cases} \tag{3.16}$$

Theorem 3.0.2. *Let p be an odd prime, $\chi_1, \ldots, \chi_s$ be mod p^m characters with at least one of them primitive, and h_1 be of the form (3.4). With n and t as in (3.7) and (3.15) we suppose that $m \geq 2t + n + 2$.*

If the $\chi_i = (\chi_i')^{k_i}$ for some primitive characters χ_i' mod p^m such that $\chi_1' \ldots \chi_s'$ is induced *by a primitive mod p^{m-n} character, and the* $A_i^{-1}B'c_i'v'^{-1} \equiv \alpha_i^{k_i} \mod p^m$ *for some* α_i*, then*

$$\mathcal{J}_1 = D_1 \cdots D_s p^{\frac{1}{2}(m(s-1)+n)} \chi_1(\alpha_1) \cdots \chi_s(\alpha_s) \delta(\chi_1', \ldots, \chi_s'), \tag{3.17}$$

where the c_i' *define the* χ_i' *as in* (3.12)*,* $v' = p^{-n}(c_1' + \cdots + c_s')$*,* $\delta(\chi_1', \ldots, \chi_s')$ *is as in* (3.11) *with* c_i' *and* v' *replacing the* c_i *and* v*.*

Otherwise $\mathcal{J}_1 = 0$*.*

The corresponding $p = 2$ result is given in Theorem 3.3.1. It is perhaps worth noting that the conditions $A_i^{-1}B'c_i'v'^{-1} \equiv \alpha_i^{k_i} \mod p^m$ for some α_i, $i = 1, \ldots, s$, lead to $D_1 \cdots D_s$ non-trivial solutions to the congruence restriction $A_1\alpha_1^{k_1} + \cdots + A_s\alpha_s^{k_s} \equiv B \bmod p^m$.

We prove the theorem in Section 3.2, but first we show that the χ_i must be k_ith powers and express $\mathcal{J}_1$ in terms Jacobi sums (3.2) and hence in terms of Gauss sums.

3.1 Writing $\mathcal{J}_1$ in Terms of Gauss Sums

We first show that $\mathcal{J}_1 = 0$ unless each χ_i is a k_ith power. We actually consider a slightly more general sum.

Lemma 3.1.1. *For any prime* p*, multiplicative characters* $\chi_1, \ldots, \chi_s, \chi$ *mod* p^m*, and* $f, g, h \in \mathbb{Z}[x_1, \ldots, x_s]$*, the sum*

$$J = \sum_{\substack{x_1=1 \\ h(x_1^{k_1}, \ldots, x_s^{k_s}) \equiv B \bmod p^m}}^{p^m} \cdots \sum_{x_s=1}^{p^m} \chi_1(x_1) \cdots \chi_s(x_s) \chi(f(x_1^{k_1}, \ldots, x_s^{k_s})) e_{p^m}(g(x_1^{k_1}, \ldots, x_s^{k_s})),$$

is zero unless $\chi_i = (\chi_i')^{k_i}$ *for some mod* p^m *characters* χ_i' *for all* $1 \le i \le s$*.*

Proof. Let p be a prime. If $z_1^{k_1} = 1$, then the change of variables $x_1 \mapsto x_1 z_1$ gives

$$J = \sum_{\substack{x_1=1 \\ h(x_1^{k_1},\ldots,x_s^{k_s}) \equiv B \bmod p^m}}^{p^m} \cdots \sum_{x_s=1}^{p^m} \chi_1(x_1 z_1) \cdots \chi_s(x_s) \chi\left(f(x_1^{k_1},\ldots,x_s^{k_s})\right) e_{p^m}\left(g(x_1^{k_1},\ldots,x_s^{k_s})\right)$$
$$= \chi_1(z_1) J.$$

Hence if $J \neq 0$ we must have $1 = \chi_1(z_1)$. For p odd we can choose $z_1 = a^{\phi(p^m)/(k_1,\phi(p^m))}$, where a is a primitive root mod p^m. Then $1 = \chi_1(z_1) = \chi_1(a)^{\phi(p^m)/(k_1,\phi(p^m))} = e^{2\pi i c_1/(k_1,\phi(p^m))}$ and $(k_1, \phi(p^m)) \mid c_1$. Hence there is an integer c_1' satisfying

$$c_1 \equiv c_1' k_1 \bmod \phi(p^m),$$

and $\chi_1 = (\chi_1')^{k_1}$ where χ_1' is the mod p^m character with $\chi_1'(a) = e_{\phi(p^m)}(c_1')$.

For $p = 2$ and $m \geq 3$ recall that $\mathbb{Z}_{2^m}^*$ needs two generators -1 and 5, where 5 has order 2^{m-2} (see for example [8]). Taking $z_1 = 5^{2^{m-2}/(k_1,2^{m-2})}$ we see that $(k_1, 2^{m-2}) \mid c_1$ and there exists a c_1' with $c_1' k_1 \equiv c_1 \bmod 2^{m-2}$. Setting

$$\chi_1'(-1) = \chi_1(-1), \quad \chi_1'(5) = e_{2^{m-2}}(c_1'),$$

we have $\chi_1(5) = (\chi_1'(5))^{k_1}$. If k_1 is odd then $\chi_1(-1) = (\chi_1'(-1))^{k_1}$. If k_1 is even then $z_1 = -1$ gives $\chi_1(-1) = 1 = (\chi_1'(-1))^{k_1}$. Hence $\chi_1 = (\chi_1')^{k_1}$.

The same technique gives $\chi_i = (\chi_i')^{k_i}$ for all $i = 1, \ldots, s$.

□

From Lemma 3.1.1 we can thus assume that the χ_i are k_ith powers, enabling us to express $J_B(\vec{\chi}, h, p^m)$ in terms of (3.2) sums and hence, by (3.9), Gauss sums.

Theorem 3.1.1. *Let $\chi_1, \ldots, \chi_s$ be mod p^m characters with $\chi_i = (\chi_i')^{k_i}$ for some mod p^m*

characters χ_i', $1 \le i \le s$, h_1 *be of the form* (3.4)*. Then,*

$$\mathcal{J}_1 = \sum_{\substack{(\chi_i'')^{k_i}=\chi_0 \\ i=1,\ldots,s}} \left(\prod_{j=1}^{s} \chi_j'\chi_j''(A_j^{-1}) \right) J_B(\chi_1'\chi_1'', \ldots, \chi_s'\chi_s'', p^m), \tag{3.18}$$

where χ_0 *is the principal character mod* p^m*.*

Recall n *is the power of* p *dividing* B *and* t *is the highest power of* p *dividing the* k_i*. If*

$$m \ge n + t + \begin{cases} 2, & \text{for } p \text{ odd}, \\ 3, & \text{for } p = 2, \end{cases}$$

and at least one of the characters is primitive mod p^m *then* $\mathcal{J}_1 = 0$ *unless all the* χ_i' *are primitive mod* p^m *with* $\chi_1' \ldots \chi_s'$ *induced by a primitive mod* p^{m-n} *character, in which case*

$$\mathcal{J}_1 = \sum_{\substack{(\chi_i'')^{k_i}=\chi_0 \\ i=1,\ldots,s}} \frac{\prod_{i=1}^{s} \chi_i'\chi_i''(A_i^{-1}B')G(\chi_i'\chi_i'', p^m)}{G(\chi_1'\chi_1'' \cdots \chi_s'\chi_s'', p^{m-n})}. \tag{3.19}$$

Proof. Write $\chi_i = (\chi_i')^{k_i}$. If $p \nmid u$ then from Lemma 2.2.2 the sum

$$\sum_{\chi^{k_i}=\chi_0 \bmod p^m} \chi(u) = D_i := \begin{cases} (k_i, \phi(p^m)), & \text{if } p \text{ is odd or } p^m = 2, 4, \\ 2(k_i, 2^{m-2}), & \text{if } p = 2,\ m \ge 3,\ k_i \text{ is even}, \\ 1, & \text{if } p = 2,\ m \ge 3,\ k_i \text{ is odd}, \end{cases} \tag{3.20}$$

if u is a k_ith power mod p^m (where each k_ith power is achieved D_i times) and equals zero otherwise.

Making the substitution $u_i \mapsto A_i^{-1}u_i$, we have

$$
\begin{aligned}
\mathcal{J}_1 &= \sum_{\substack{x_1=1 \\ A_1x_1^{k_1}+\cdots+A_sx_s^{k_s}\equiv B \bmod p^m}}^{p^m} \cdots \sum_{x_s=1}^{p^m} \chi_1'(x_1^{k_1})\cdots\chi_s'(x_s^{k_s}) \\
&= \sum_{\substack{(\chi_i'')^{k_i}=\chi_0 \\ i=1,\dots,s}} \sum_{\substack{u_1=1 \\ A_1u_1+\cdots+A_su_s\equiv B \bmod p^m}}^{p^m} \cdots \sum_{u_s=1}^{p^m} \chi_1'\chi_1''(u_1)\cdots\chi_s'\chi_s''(u_s) \\
&= \sum_{\substack{(\chi_i'')^{k_i}=\chi_0 \\ i=1,\dots,s}} \overline{\chi_1'\chi_1''}(A_1)\cdots\overline{\chi_s'\chi_s''}(A_s) \sum_{\substack{u_1=1 \\ u_1+\cdots+u_s\equiv B \bmod p^m}}^{p^m} \cdots \sum_{u_s=1}^{p^m} \chi_1'\chi_1''(u_1)\cdots\chi_s'\chi_s''(u_s),
\end{aligned}
\tag{3.21}
$$

and (3.18) is clear. Note, if χ_i is primitive mod p^m then $\chi_i'\chi_i''$ must be primitive for all χ_i'' mod p^m with $(\chi_i'')^{k_i} = \chi_0$ (since $\chi_i = (\chi_i'\chi_i'')^{k_i}$).

Hence, by (3.9), if $m > n$ and at least one of the χ_i is primitive mod p^m

$$
\mathcal{J}_1 = p^{-(m-n)} \sum_{\substack{(\chi_i'')^{k_i}=\chi_0 \\ i=1,\dots,s}}^{*} \overline{G\left(\prod_{j=1}^{s} \chi_j'\chi_j'', p^{m-n}\right)} \prod_{i=1}^{s} \chi_i'\chi_i''(A_i^{-1}B')G\left(\chi_i'\chi_i'', p^m\right), \tag{3.22}
$$

where the * indicates the sum is restricted to the χ_i'' mod p^m such that $\prod_{j=1}^{s}\chi_j'\chi_j''$ is a mod p^{m-n} character. Suppose further that $m \geq n+t+2$ and p is odd. Since $(\chi_i'')^{k_i} = \chi_0$, that is $e_{\phi(p^m)}(c_i''k_i) = 1$, and $p^{t_i} \parallel k_i$, then

$$
p^{m-t_i-1} \mid c_i'' \quad \Rightarrow \quad p^{n+1} \mid c_i''. \tag{3.23}
$$

Likewise for $p = 2$, if $(\chi_i'')^{k_i} = \chi_0$ and $m \geq n+t+3$, we have

$$
2^{m-t-2} | c_i'' \quad \Rightarrow \quad 2^{n+1} | c_i''. \tag{3.24}
$$

Hence $p \mid (c_i' + c_i'')$ iff $p \mid c_i'$ and $p^n \parallel \sum_{i=1}^{s}(c_i' + c_i'')$ iff $p^n \parallel \sum_{i=1}^{s} c_i'$. That is $\chi_i'\chi_i''$ is primitive mod p^m iff χ_i' is primitive mod p^m and $\prod_{i=1}^{s}\chi_i'\chi_i''$ is primitive mod p^{m-n} iff $\prod_{i=1}^{s}\chi_i'$

is primitive mod p^{m-n}. Observing that for $k \geq 2$ we have $G(\chi, p^k) = 0$ if χ is not primitive mod p^k we see that all the terms in (3.22) will be zero unless the χ_i' are all primitive mod p^m with $\prod_{i=1}^s \chi_i'$ primitive mod p^{m-n}. Observing that $|G(\chi, p^k)|^2 = p^k$ if χ is primitive mod p^k gives the form (3.19).

□

3.2 Proof of Theorem 3.0.2

Suppose that $m \geq n+t+2$ and at least one of the χ_i is primitive. From Lemma 3.1.1 and Theorem 3.1.1 we can assume that the $\chi_i = (\chi_i')^{k_i}$ with the χ_i' primitive mod p^m and $\prod_{i=1}^s \chi_i'$ primitive mod p^{m-n}, else the sum is zero. As in the proof of Theorem 3.1.1 we know that all the $\chi_i'\chi_i''$ are primitive mod p^m with $\prod_{i=1}^s \chi_i'\chi_i''$ primitive mod p^{m-n}. Hence using (3.18) and the evaluation (3.10) from [15] we can write

$$\mathcal{J}_1 = p^{\frac{1}{2}(m(s-1)+n)} \sum_{(\chi_i'')^{k_i}=\chi_0} \frac{\chi_1'\chi_1''(A_1^{-1}B'(c_1'+c_1'')) \cdots \chi_s'\chi_s''(A_s^{-1}B'(c_s'+c_s''))}{\chi_1'\chi_1'' \cdots \chi_s'\chi_s''(v)} \tilde{\delta}, \tag{3.25}$$

where the

$$\chi_i'\chi_i''(a) = e_{\phi(p^m)}(c_i'+c_i''), \quad v = p^{-n}\sum_{i=1}^s (c_i'+c_i''),$$

and

$$\tilde{\delta} = \delta(\chi_1'\chi_1'', \ldots, \chi_s'\chi_s'') = \left(\frac{-2r}{p}\right)^{m(s-1)+n} \left(\frac{v}{p}\right)^{m-n} \left(\frac{\prod_{i=1}^s (c_i'+c_i'')}{p}\right)^m \varepsilon_{p^m}^s \varepsilon_{p^{m-n}}^{-1},$$

with ε_{p^m}, and r as defined in (3.13) and (3.12), with an extra factor $e_3(rv)$ needed when $p = m-n = 3$. From (3.23) we know that $p^{n+1} \mid c_i''$ for all i, so $c_i'+c_i'' \equiv c_i'$ mod p, $v \equiv v'$ mod p, and

$$\tilde{\delta} = \delta(\chi_1'\chi_1'', \ldots, \chi_s'\chi_s'') = \delta(\chi_1', \ldots, \chi_s'),$$

and so may be pulled out of the sum straight away. Suppose now that

$$m \geq n + 2t + 2. \tag{3.26}$$

It is perhaps worth noting that in [18] the sums (3.6) genuinely required a different evaluation in the range $n + t + 2 \leq m < n + 2t + 2$ to that when $m \geq n + 2t + 2$. Since $p^{m-1-t_i} \mid c_i''$ we certainly have $p^{m-1-t} \mid c_i''$ and the characters χ_i'' and $\prod_{i=1}^{s} \chi_i''$ are mod p^{t+1} characters. Condition (3.26) ensures $p^{t+n+1} \mid c_i''$, $v \equiv v'$ mod p^{t+1} and

$$\chi_i''(c_i' + c_i'') = \chi_i''(c_i'), \qquad \chi_1'' \cdots \chi_s''(v) = \chi_1'' \cdots \chi_s''(v'). \tag{3.27}$$

We define the integers R_j by

$$a^{\phi(p^j)} = 1 + R_j p^j. \tag{3.28}$$

Since $(1 + R_{i+1}p^{i+1}) = (1 + R_i p^i)^p$ we readily obtain $R_{i+1} \equiv R_i$ mod p^i and $R_j \equiv R_i$ mod p^i for all $j \geq i$. Defining positive integers l_i with

$$l_i = (c_i')^{-1}(c_i'' p^{-(m-t-1)}) R_{m-t-1}^{-1} \bmod p^m,$$

and noting that $2(m - t - 1) \geq m$ we have

$$\begin{aligned} c_i' + c_i'' &\equiv c_i' \left(1 + l_i R_{m-t-1} p^{m-t-1}\right) \bmod p^m \\ &\equiv c_i' \left(1 + R_{m-t-1} p^{m-t-1}\right)^{l_i} \bmod p^m \\ &\equiv c_i' a^{l_i \phi(p^{m-t-1})} \bmod p^m, \end{aligned}$$

and $\chi_i'(c_i' + c_i'') = \chi_i'(c_i') e_{p^{t+1}}(c_i' l_i)$.

Since $m-t-n-1 \geq t+1$ we have $R_{m-t-1} \equiv R_{m-t-n-1} \bmod p^{t+1}$ and

$$\prod_{i=1}^{s} \chi_i' \chi_i''(c_i' + c_i'') = e_{p^{t+1}}(L) \prod_{i=1}^{s} \chi_i' \chi_i''(c_i'), \quad L := R_{m-t-n-1}^{-1} \sum_{i=1}^{s} c_i'' p^{-(m-t-1)}. \tag{3.29}$$

Similarly, noting that $2(m-n-t-1) \geq m-n$,

$$\begin{aligned} v &= v' + p^{-n}(c_1'' + \cdots + c_s'') \\ &\equiv v' \left(1 + (v')^{-1} L R_{m-n-t-1} p^{m-n-t-1}\right) \bmod p^m \\ &\equiv v' a^{(v')^{-1}\phi(p^{m-t-n-1})L} \quad \bmod p^{m-n}, \end{aligned}$$

and

$$\begin{aligned} \chi_1'\chi_1'' \cdots \chi_s'\chi_s''(v) &= \chi_1'\chi_1'' \cdots \chi_s'\chi_s''(v') e_{\phi(p^m)}(p^n v'(v')^{-1}\phi(p^{m-t-n-1})L) \\ &= \chi_1'\chi_1'' \cdots \chi_s'\chi_s''(v') e_{p^{t+1}}(L). \end{aligned} \tag{3.30}$$

By substituting (3.29) and (3.30) in (3.25) we get

$$\begin{aligned} \mathcal{J}_1 &= p^{\frac{1}{2}(m(s-1)+n)} \delta(\chi_1', \ldots, \chi_s') \sum_{\substack{(\chi_i'')^{k_i} = \chi_0 \\ i=1,\ldots,s}} \frac{\chi_1'\chi_1''(A_1^{-1}B'c_1') \cdots \chi_s'\chi_s''(A_s^{-1}B'c_s')}{\chi_1'\chi_1'' \cdots \chi_s'\chi_s''(v')} \\ &= p^{\frac{1}{2}(m(s-1)+n)} \delta(\chi_1', \ldots, \chi_s') \prod_{j=1}^{s} \chi_j'(A_j^{-1}B'c_j'v'^{-1}) \prod_{i=1}^{s} \sum_{(\chi_i'')^{k_i}=\chi_0} \chi_i''(A_i^{-1}B'c_i'v'^{-1}). \end{aligned} \tag{3.31}$$

Clearly this sum is zero unless each $A_i^{-1}B'c_i'v'^{-1}$ is a k_i-th power, when

$$\mathcal{J}_1 = D_1 \cdots D_s p^{\frac{1}{2}(m(s-1)+n)} \delta(\chi_1', \ldots, \chi_s') \prod_{i=1}^{s} \chi_i'(A_i^{-1}B'c_i'v'^{-1}). \quad \square$$

3.3 The Case $p = 2$

As shown in [15] the sums (3.2) still have an evaluation (3.10) when $p = 2$ and $m - n \geq 5$, with δ now defined by

$$\delta(\chi_1, \ldots, \chi_s) = \left(\frac{2}{v}\right)^{m-n} \left(\frac{2}{c_1 \cdots c_s}\right)^m \omega^{(2^n-1)v}, \tag{3.32}$$

where c_i, v, and ω are defined as

$$\chi_i(5) = e_{2^{m-2}}(c_i), \quad 1 \leq c_i \leq 2^{m-2}, \quad 1 \leq i \leq s, \tag{3.33}$$

and

$$v = 2^{-n}(c_1 + \cdots + c_s), \quad \omega := e^{\pi i/4}. \tag{3.34}$$

Theorem 3.3.1. *Let $\chi_1, \ldots, \chi_s$ be mod 2^m characters with at least one of them primitive, and h_1 be of the form (3.4). Suppose that $m \geq 2t + n + 5$.*

If the $\chi_i = (\chi_i')^{k_i}$ for some primitive characters χ_i' mod 2^m such that $\chi_1' \ldots \chi_s'$ is induced by a primitive mod 2^{m-n} character, and the $A_i^{-1}B'c_i'v'^{-1} \equiv \alpha_i^{k_i} \mod 2^m$ for some α_i, then

$$\mathcal{J}_1 = 2^{\frac{1}{2}(m(s-1)+n)} D_1 \cdots D_s \, \chi_1(\alpha_1) \cdots \chi_s(\alpha_s) \delta(\chi_1', \ldots, \chi_s'), \tag{3.35}$$

where the c_i' are defined by $\chi_i'(5) = e_{2^{m-2}}(c_i')$, $v' = 2^{-n}\sum_{i=1}^{s} c_i'$ and $\delta(\chi_1', \ldots, \chi_s')$ is as in (3.32) with c_i' and v' replacing the c_i and v.

Otherwise $\mathcal{J}_1 = 0$.

Proof. Suppose first that $m \geq n + t + 5$ and at least one of the χ_i primitive mod 2^m. From Lemma 3.1.1 and Theorem 3.1.1 we can assume that $\chi_i = (\chi_i')^{k_i}$ with χ_i' primitive mod 2^m and $\prod_{i=1}^{s} \chi_i'$ primitive mod 2^{m-n}, else the sum is zero. As in the proof of Theorem 3.1.1 we know that $\chi_i'\chi_i''$ is primitive mod 2^m and $\prod_{i=1}^{s} \chi_i'\chi_i''$ is primitive mod 2^{m-n}. Hence using

(3.18) and the evaluation for case $p=2$ from [15] we can write

$$\mathcal{J}_1 = 2^{\frac{1}{2}(m(s-1)+n)} \sum_{(\chi_i'')^{k_i}=\chi_0} \frac{\chi_1'\chi_1''(A_1^{-1}B'(c_1'+c_1''))\cdots\chi_s'\chi_s''(A_s^{-1}B'(c_s'+c_s''))}{\chi_1'\chi_1''\cdots\chi_s'\chi_s''(v)}\tilde{\delta}, \tag{3.36}$$

where the

$$\chi_i'\chi_i''(5) = e_{2^{m-2}}(c_i'+c_i''), \quad v = 2^{-n}\sum_{i=1}^{s}(c_i'+c_i''),$$

and

$$\tilde{\delta} = \delta(\chi_1'\chi_1'',\ldots,\chi_s'\chi_s'') = \left(\frac{2}{v}\right)^{m-n}\left(\frac{2}{\prod_{i=1}^{s}(c_i'+c_i'')}\right)^{m}\omega^{(2^n-1)v}.$$

From $(\chi_i'')^{k_i}=1$ we have $e_{2^{m-2}}(c_i''k_i)=1$ and $2^{m-t-2}|c_i''$. Hence

$$c_i'+c_i'' \equiv c_i' \bmod 2^{m-t-2}, \tag{3.37}$$

and

$$v = 2^{-n}\sum_{i=1}^{s}(c_i'+c_i'') \equiv 2^{-n}\sum_{i=1}^{s}c_i' = v' \bmod 2^{m-n-t-2}. \tag{3.38}$$

So for $m \geq n+t+5$ we have $c_i'+c_i'' \equiv c_i' \bmod 8$, $v \equiv v' \bmod 8$, giving

$$\left(\frac{2}{c_i'+c_i''}\right) = \left(\frac{2}{c_i'}\right), \quad \left(\frac{v}{p}\right) = \left(\frac{v'}{p}\right), \quad \omega^{(2^n-1)v} = \omega^{(2^n-1)v'},$$

and $\tilde{\delta} = \delta(\chi_1'\chi_1'',\ldots,\chi_s'\chi_s'') = \delta(\chi_1',\ldots,\chi_s')$. From $2^{m-t-2} \mid c_i''$ we know that the χ_i'' are all mod 2^{t+2} characters. Suppose now that $m \geq 2t+n+4$. Then (3.37) and (3.38) give $c_i'+c_i'' \equiv c_i' \bmod 2^{t+2}$, $v \equiv v' \bmod 2^{t+2}$, and

$$\chi_i''(c_i'+c_i'') = \chi_i''(c_i'), \quad \chi_1''\cdots\chi_s''(v) = \chi_1''\cdots\chi_s''(v').$$

For $p=2$ we define the integers $R_j, j \geq 2$ by

$$5^{2^{j-2}} = 1 + Rj2^j.$$

From $R_{i+1} \equiv R_i + 2^{i-1}R_i^2$ we have the relationship $R_j \equiv R_i \bmod 2^{i-1}$ for all $j \geq i \geq 2$. Define a positive integer $l_i := (c_i')^{-1}c_i''2^{-(m-t-2)}R_{m-t-2}^{-1} \bmod 2^m$. Since $2(m-t-2) \geq m$ we have

$$\begin{aligned} c_i' + c_i'' &\equiv c_i'\left(1 + l_i R_{m-t-2}2^{m-t-2}\right) \bmod 2^m \\ &\equiv c_i'\left(1 + R_{m-t-2}2^{m-t-2}\right)^{l_i} \bmod 2^m \\ &\equiv c_i' 5^{l_i 2^{m-t-4}} \bmod 2^m, \end{aligned}$$

and $\chi_i'(c_i' + c_i'') = \chi_i'(c_i')e_{2^{t+2}}(c_i' l_i)$. If $m \geq 2t + n + 5$, then

$$R_{m-t-2} \equiv R_{m-t-n-2} \bmod 2^{m-t-n-3} \equiv R_{m-t-n-2} \bmod 2^{t+2}$$

giving

$$\prod_{i=1}^{s} \chi_i'\chi_i''(c_i' + c_i'') = e_{2^{t+2}}(L)\prod_{i=1}^{s}\chi_i'\chi_i''(c_i'), \quad L := R_{m-t-n-2}^{-1}\sum_{i=1}^{s} c_i''2^{-(m-t-2)}. \tag{3.39}$$

Similarly, since $2(m-n-t-2) \geq m-n$,

$$\begin{aligned} v &= v' + 2^{-n}(c_1'' + \cdots + c_s'') \\ &\equiv v'\left(1 + (v')^{-1}LR_{m-n-t-2}2^{m-n-t-2}\right) \\ &\equiv v'5^{(v')^{-1}2^{m-t-n-4}L} \qquad \bmod 2^{m-n}, \end{aligned}$$

and

$$\chi_1'\chi_1''\cdots\chi_s'\chi_s''(v) = \chi_1'\chi_1''\cdots\chi_s'\chi_s''(v')e_{2^{t+2}}(L). \tag{3.40}$$

By substituting (3.39) and (3.40) in (3.36) we get (3.31) and the rest of the proof follows unchanged from p odd.

□

3.4 Imprimitive Characters

We assumed in Theorem 3.0.2 that at least one of the characters is primitive mod p^m. This is a fairly natural assumption. For example if $p \nmid k_i$ for at least one i and none of the χ_i are primitive mod p^m then we can reduce to a mod p^{m-1} sum.

Lemma 3.4.1. *Let p be an odd prime and h_1 be of the form (3.4). If $\chi_1, \ldots, \chi_s$ are imprimitive characters mod p^m with $p \nmid k_i$ for some i and $m \geq 2$, then*

$$J_B(\vec{\chi}, h_1, p^m) = p^{s-1} J_B(\vec{\chi}, h_1, p^{m-1}).$$

Proof. Suppose that $\chi_1, \ldots, \chi_s$ are p^{m-1} characters with $p \nmid k_i$ for some i. Writing $x_i = u_i + v_i p^{m-1}$, with $u_i = 1, \ldots, p^{m-1}$ and $v_i = 1, \ldots, p$ gives

$$J_B(\vec{\chi}, h_1, p^m) = \sum_{\substack{u_1,\ldots,u_s=1 \\ \sum_{i=1}^s A_i(u_i+v_ip^{m-1})^{k_i} \equiv B \bmod p^m}}^{p^{m-1}} \sum_{v_1,\ldots,v_s=1}^{p} \chi_1(u_1)\cdots\chi_s(u_s),$$

where the $\chi_i(u_i)$ allow us to restrict to $(u_i, p) = 1$. Expanding we see that

$$\sum_{i=1}^s A_i(u_i + v_i p^{m-1})^{k_i} \equiv \sum_{i=1}^s A_i u_i^{k_i} + p^{m-1}\left(\sum_{i=1}^s A_i k_i u_i^{k_i-1} v_i\right) \equiv B \bmod p^m, \tag{3.41}$$

as long as $m \geq 2$. Thus the u_i must satisfy

$$\sum_{i=1}^s A_i u_i^{k_i} \equiv B \bmod p^{m-1}, \tag{3.42}$$

and for any $u_1, \ldots, u_s$ satisfying (3.42), to satisfy (3.41) the v_i must satisfy

$$\sum_{i=1}^s A_i k_i u_i^{k_i-1} v_i \equiv p^{-(m-1)}\left(B - \sum_{i=1}^s A_i u_i^{k_i}\right) \bmod p. \tag{3.43}$$

If p does not divide one of the exponents, $p \nmid k_1$ say, then for each of the p^{s-1} choices of $v_2, \ldots, v_s$ there will be exactly one v_1 satisfying (3.43)

$$v_1 \equiv \left(p^{-(m-1)} \left(B - \sum_{i=1}^{s} A_i u_i^{k_i} \right) - \sum_{i=2}^{s} A_i k_i u_i^{k_i - 1} v_i \right) \left(A_1 k_1 u_1^{k_1 - 1} \right)^{-1} \bmod p,$$

and

$$J_B(\vec{\chi}, h_1, p^m) = p^{s-1} \sum_{\substack{u_1, \ldots, u_s = 1 \\ \sum_{i=1}^{s} A_i u_i^{k_i} \equiv B \bmod p^{m-1}}}^{p^{m-1}} \chi_1(u_1) \cdots \chi_s(u_s) = p^{s-1} J_B(\vec{\chi}, h_1, p^{m-1}).$$

□

If the χ_i are all imprimitive mod p^m and $p \mid k_i$ for all i then we still reduce to a mod p^{m-1} sum, but as with a Heilbronn sum it seems unlikely that there is a nice evaluation:

$$J_B(\vec{\chi}, h_1, p^m) = p^s \sum_{\substack{x_1 = 1 \\ A_1 x_1^{k_1} + \cdots + A_s x_s^{k_s} \equiv B \bmod p^m}}^{p^{m-1}} \cdots \sum_{x_s = 1}^{p^{m-1}} \chi_1(x_1) \cdots \chi_s(x_s).$$

Chapter 4

Character Sums with an Explicit Evaluation

Let $\vec{\chi} = (\chi, \chi_1, \ldots, \chi_s)$ denote $s+1$ multiplicative Dirichlet characters mod q. For an $h \in \mathbb{Z}[x_1, \ldots, x_s]$ we define the complete character sum

$$J(\vec{\chi}, h, q) := \sum_{x_1=1}^{q} \cdots \sum_{x_s=1}^{q} \chi_1(x_1) \cdots \chi_s(x_s) \chi(h(x_1, \ldots, x_s)). \tag{4.1}$$

From Lemma 2.1.2 in Chapter 2 we see that if $(r, s) = 1$, then splitting the mod rs characters χ_i into mod r and mod s characters χ_i', χ_i'', that is $\chi_i = \chi_i' \chi_i''$,

$$J(\vec{\chi}, h, rs) = J(\vec{\chi'}, h, r) J(\vec{\chi''}, h, s).$$

Hence, we shall restrict our attention to prime power moduli $q = p^m$. When $m \geq 2$, methods of Cochrane [5] (see also Cochrane and Zheng [6] & [7]) can be used to simplify the sums and in some special cases obtain an explicit evaluation. For example, the sum

$$\sum_{x=1}^{p^m} \chi_1(x) \chi_2(Ax^k + B) \tag{4.2}$$

was evaluated in [18] (p odd) and [19] ($p=2$) for m sufficiently large (for $m \geq 2$ if $p \nmid 2ABk$). In [15] an evaluation was obtained for the Jacobi type sums

$$h(x_1,\ldots,x_s)=x_1+\cdots+x_s+B, \tag{4.3}$$

and in Chapter 3 for their generalization

$$h_1(x_1,\ldots,x_s)=A_1x_1^{k_1}+\cdots+A_sx_s^{k_s}+B, \quad p\nmid A_1\cdots A_s,$$

for m sufficiently large (for $m \geq 2$ when $p \nmid 2Bk_1\cdots k_s$). Zhang and Wang recently showed in [22] that (4.1) has an explicit evaluation when

$$h(x_1,\ldots,x_s)=x_1+\cdots+x_s+Bx_1^{-1}\cdots x_s^{-1}, \quad p\nmid B,$$

with $\chi_i=\chi_0$, the principal character mod p^m, and

$$s=2^N-1, \;\; m \text{ even}, \;\; p\equiv 3 \pmod 4, \;\; \chi(-1)=1. \tag{4.4}$$

In this chapter we will consider the sum (4.1) for the more general

$$h(x_1,\ldots,x_s)=A_1x_1+\cdots+A_sx_s+Bx_1^{w_1}\cdots x_s^{w_s}, \quad p\nmid A_1\cdots A_s, \tag{4.5}$$

where the w_i are arbitrary integers, and obtain an evaluation when m is sufficiently large, for $m\geq 2$ if $p\nmid 2Bk$ where

$$k:=1-w_1-\cdots-w_s. \tag{4.6}$$

In particular, we shall see that the conditions (4.4) are not needed. Note, if we use the change of variables $x_i \mapsto x_i A_i^{-1}$ for all $i = 1, \ldots, s$, then for h of the form (4.5),

$$J(\vec{\chi}, h, p^m) = \overline{\chi_1}(A_1) \cdots \overline{\chi_s}(A_s) J(\vec{\chi}, x_1 + \cdots + x_s + BA_1^{-w_1} \cdots A_s^{-ws} x_1^{w_1} \cdots x_s^{w_s}, p^m).$$

Hence it is enough here to consider

$$h_2 = h_2(x_1, \ldots, x_s) := x_1 + \cdots + x_s + Bx_1^{w_1} \cdots x_s^{w_s} \tag{4.7}$$

and evaluate the sum

$$\mathcal{J}_2 := J(\vec{\chi}, h_2, p^m) = \sum_{x_1=1}^{p^m} \cdots \sum_{x_s=1}^{p^m} \chi_1(x_1) \cdots \chi_s(x_s) \chi(x_1 + \cdots + x_s + Bx_1^{w_1} \cdots x_s^{w_s}). \tag{4.8}$$

We use n and t to denote the power of p dividing B and k,

$$B = p^n B_1, \;\; p \nmid B_1, \;\; p^t \mid\mid k. \tag{4.9}$$

To obtain our evaluation we shall first show in §2 that the sum is zero unless

$$\chi \chi_1 \cdots \chi_s = \chi_*^k, \tag{4.10}$$

for some mod p^{m-n} character χ_*. In §3 we write our sums in terms of Gauss sums, and then in §4 we use the explicit evaluation of Gauss sums from [15] to obtain the evaluation stated in Theorem 4.0.1 below. When p is odd, we suppose that a is a primitive root mod p^m. Writing

$$e_q(x) := e^{2\pi i x/q}, \tag{4.11}$$

we define integers $r := (a^{p-1}-1)/p$, $1 \le c, c_i \le \phi(p^m)$, and $1 \le c_* \le \phi(p^{m-n})$, by

$$\chi(a) = e_{\phi(p^m)}(c), \quad \chi_i(a) = e_{\phi(p^m)}(c_i), \quad \chi_*(a) = e_{\phi(p^{m-n})}(c_*). \tag{4.12}$$

When $p = 2$, we similarly define the integers $1 \le c, c_i \le 2^{m-2}$, $1 \le c_* \le 2^{m-n-2}$ by

$$\chi(5) = e_{2^{m-2}}(c), \quad \chi_i(5) = e_{2^{m-2}}(c_i), \quad \chi_*(5) = e_{2^{m-n-2}}(c_*). \tag{4.13}$$

Define also λ and ε_{p^m} as

$$\lambda := -B_1 \prod_{i=1}^{s} \left(c_i c_*^{-1} + p^n w_i\right)^{w_i} \mod p^m, \quad \varepsilon_{p^m} := \begin{cases} 1, \text{ if } p^m \equiv 1 \mod 4, \\ i, \text{ if } p^m \equiv 3 \mod 4. \end{cases} \tag{4.14}$$

Theorem 4.0.1. *Let p be a prime and $\chi, \chi_1, \ldots, \chi_s$ be mod p^m characters with χ primitive. Let h_2 be of the form (4.7) and n, k, t be as in (4.6) and (4.9). Suppose that*

$$m \ge 2t + n + 3\beta - 1, \quad \beta := \begin{cases} 1, & \text{if } p \text{ is odd,} \\ 2, & \text{if } p = 2. \end{cases} \tag{4.15}$$

If $\chi\chi_1 \cdots \chi_s = \chi_*^k$ for some primitive mod p^{m-n} character χ_* such that the $\chi_i \chi_*^{w_i}$ are all primitive characters mod p^m and λ, defined in (4.14), is a kth power mod p^{m-n}, then

$$\mathcal{J}_2 = (k, p-1) p^{\frac{ms+n}{2}+\alpha} \delta\, \chi_*(\lambda) \chi\left(\sum_{i=1}^{s} c_i c_*^{-1} - p^n k\right) \prod_{i=1}^{s} \chi_i(c_i c_*^{-1} + w_i p^n),$$

where

$$\delta := \left(\frac{2r}{p}\right)^{sm-n} \left(\frac{-1}{p}\right)^{sm} \left(\frac{c_*^{m-n} c^m \prod_{i=1}^{s}(c_i + w_i p^n c_*)^m}{p}\right) \varepsilon_{p^m}^{s-1} \varepsilon_{p^{m-n}} \tag{4.16}$$

for p odd, unless $p^{m-n}=3^3$, $n>0$ when an extra factor $e_3(rc_*)$ is needed,

$$\delta := \left(\frac{2}{c_*^{m-n}c^m\prod_{i=1}^{s}(c_i+w_i2^nc_*)^m}\right)e_8((2^n-1)c_*) \tag{4.17}$$

for $p=2$, and

$$\alpha := \begin{cases} t, & \text{if } p \text{ is odd, or } p=2 \text{ and } t=0,\\ t+1, & \text{if } p=2 \text{ and } t\geq 1, \end{cases} \tag{4.18}$$

with c_i, c, c_* and ε_{p^m} as defined in (4.12), (4.13) and (4.14).

Otherwise $\mathcal{J}_2=0$.

4.1 Preliminaries

We first observe that it is natural to assume that χ is a primitive character mod p^m. If all the χ_i and χ are imprimitive mod p^m, then for any polynomial h we can simply reduce (4.1) to a mod p^{m-1} sum, $J(\vec{\chi},h,p^m)=p^sJ(\vec{\chi},h,p^{m-1})$. If some χ_i is primitive, then there is a $u\equiv 1 \bmod p^{m-1}$ with $\chi_i(u)\neq 1$, and if χ is imprimitive mod p^m, then the change of variable $x_i\mapsto x_iu$ gives $J(\vec{\chi},h,p^m)=\chi_i(u)J(\vec{\chi},h,p^m)$, and so $J(\vec{\chi},h,p^m)=0$.

It also seems natural to assume that n satisfies

$$m\geq n+\beta. \tag{4.19}$$

If $n\geq m$ or $n=m-1$ when $p=2$, then as we will show in the proof of Lemma 4.1.1,

$$J(\vec{\chi},h_2,p^m)=\begin{cases} \phi(p^m)J(\vec{\chi}_\xi,h_\xi,p^m), & \text{if } \chi\chi_1\cdots\chi_s=\chi_0,\\ 0, & \text{if } \chi\chi_1\cdots\chi_s\neq\chi_0, \end{cases} \tag{4.20}$$

where χ_0 is the principal character mod p^m, and $\vec{\chi}_\xi := (\chi,\chi_1,\ldots,\chi_{s-1})$ and

$h_\xi := x_1 + \cdots + x_{s-1} + 1 + B$ have one less variable.

The following lemma shows that $\mathcal{J}_2 = 0$ unless $\chi\chi_1 \cdots \chi_s$ is a k-th power of a mod p^{m-n} character.

Lemma 4.1.1. *For a prime p and multiplicative characters $\chi, \chi_1, \ldots, \chi_s$ mod p^m, a sum of the form (4.8) is zero unless $\chi\chi_1 \cdots \chi_s = \chi_*^k$ for some mod p^{m-n} character χ_* if (4.19) holds or $\chi\chi_1 \cdots \chi_s = \chi_0$ if (4.19) does not hold.*

Proof. Observe that if $z^k \equiv 1 \bmod p^{m-n}$, then the change of variables $x_i \mapsto x_i z$, $1 \le i \le s$, gives

$$\begin{aligned} J(\vec{\chi}, h_2, p^m) &= \sum_{x_1=1}^{p^m} \cdots \sum_{x_s=1}^{p^m} \chi\chi_1 \cdots \chi_s(z)\chi_1(x_1) \cdots \chi_s(x_s)\chi(x_1 + \cdots + x_s + Bx_1^{w_1} \cdots x_s^{w_s} z^{-k}) \\ &= \tilde{\chi}(z) J(\vec{\chi}, h_2, p^m), \end{aligned}$$

and so $J(\vec{\chi}, h_2, p^m) = 0$ unless $\tilde{\chi}(z) := \chi\chi_1 \cdots \chi_s(z) = 1$.

For p an odd prime and $n < m$, we can choose $z = a^{\phi(p^{m-n})/(k,\phi(p^{m-n}))}$ where a is a primitive root mod p^m. Hence if $J(\vec{\chi}, h_2, p^m) \neq 0$, we must have

$$1 = \tilde{\chi}(z) = \tilde{\chi}(a)^{\phi(p^{m-n})/(k,\phi(p^{m-n}))} = e^{2\pi i(\tilde{c}/p^n(k,\phi(p^{m-n}))}$$

and $p^n(k, \phi(p^{m-n})) \mid \tilde{c}$. Hence there is an integer c_* satisfying $p^n k c_* \equiv \tilde{c} \bmod \phi(p^m)$, and $\tilde{\chi} = \chi_*^k$ where χ_* is the mod p^{m-n} character with $\chi_*(a) = e_{\phi(p^{m-n})}(c_*)$.

For $p = 2$ and $m \ge n + 2$, taking $z = 5^{2^{m-n-2}/(k,2^{m-n-2})}$ and writing $\tilde{\chi}(5) = e_{2^{m-2}}(\tilde{c})$, we similarly obtain that $2^n(k, 2^{m-n-2}) \mid \tilde{c}$ and $2^n k c_* \equiv \tilde{c} \bmod 2^{m-2}$ has a solution c_*. Setting

$$\chi_*(5) = e_{2^{m-n-2}}(c_*), \quad \chi_*(-1) = \tilde{\chi}(-1),$$

we have $\tilde{\chi}(5) = \chi_*(5)^k$. If k is even, then taking $z = -1$ gives $\tilde{\chi}(-1) = 1$ (hence $\tilde{\chi}(-1) = \chi_*(-1)^k$) and in all cases $\tilde{\chi} = \chi_*^k$ where χ_* is a mod 2^{m-n} character.

If (4.19) does not hold, then we can take any z with $p \nmid z$ and $J(\vec{\chi}, h_2, p^m) = 0$ or $\tilde{\chi} = \chi_0$. If $\tilde{\chi} = \chi_0$, then the substitution $x_i \mapsto x_i x_s$ for all $i < s$ gives the expression (4.20).

□

Lemma 4.1.1 is readily generalized. For example if $g_i, h_j \in \mathbb{Z}[x_1, \ldots, x_s]$ are homogeneous with degrees k_i, d_j respectively, and (4.19) holds, then the sum

$$J := \sum_{x_1=1}^{q} \cdots \sum_{x_s=1}^{q} \chi_1(g_1) \cdots \chi_l(g_l) \chi(h_1 + Bh_2)$$

is zero unless $\chi_1^{k_1} \cdots \chi_l^{k_l} \chi^{d_1}$ is a $(d_2 - d_1)$-th power of a mod p^{m-n} character (if $z^{d_2 - d_1} \equiv 1 \bmod p^{m-n}$, then $x_i \mapsto z x_i$ gives $J = \chi_1^{k_1} \cdots \chi_l^{k_l} \chi^{d_1}(z) J$).

4.2 Writing $\mathcal{J}_2$ in Terms of Gauss Sums

For a character χ mod p^m one defines the classical Gauss sum

$$G(\chi, p^m) := \sum_{x=1}^{p^m} \chi(x) e_{p^m}(x). \tag{4.21}$$

From Lemma 4.1.1 we can assume that $\chi\chi_1 \cdots \chi_s$ is a kth power (otherwise the sum is zero), enabling us to express (4.8) in terms of Gauss sums. Similar expressions were obtained for the binomial character sums (4.2) in [18, Theorem 2.2] and the Jacobi sums (4.3) in [15, Theorem 2.2].

Theorem 4.2.1. *Let $\chi, \chi_1, \ldots, \chi_s$ be mod p^m characters with χ primitive. Let h_2 be of the form (4.7) with n, B_1 and t as defined in (4.9) and satisfying (4.19). Suppose that $\chi\chi_1 \cdots \chi_s = \chi_*^k$ for some mod p^{m-n} character χ_*. Then*

$$\mathcal{J}_2 = p^n \sum_{\chi'' \in \mathcal{Y}} \chi''\chi_*(B_1) \frac{G(\overline{\chi''\chi_*}, p^{m-n}) \prod_{i=1}^{s} G(\chi_i (\chi''\chi_*)^{w_i}, p^m)}{G(\overline{\chi}, p^m)}, \tag{4.22}$$

where $\mathcal{Y}$ denotes the mod p^{m-n} characters χ'' with $(\chi'')^k = \chi_0$.

In particular, if

$$m > n + t + \beta, \tag{4.23}$$

then $\mathcal{J}_2 = 0$ unless χ_* is a primitive mod p^{m-n} character and the $\chi_i \chi_*^{w_i}$ are all primitive mod p^m characters.

Proof. If χ is a primitive character mod p^m, then

$$G(y) := \sum_{x=1}^{p^m} \overline{\chi}(x) e_{p^m}(xy) = \chi(y) G(\overline{\chi}, p^m). \tag{4.24}$$

for any y, If $p \nmid y$, this is clear from $x \mapsto xy^{-1}$. If $p \mid y$, then taking $u \equiv 1 \mod p^{m-1}$ with $\chi(u) \neq 1$, the change of variable $x \mapsto xu$ gives $G(y) = \overline{\chi}(u) G(y)$, and so $G(y) = 0$. Thus for χ primitive, applying (4.24) with $y = h(x_1, \ldots, x_s)$, followed by change of variables $x_i \mapsto x_i x^{-1}$ and the substitution $\chi \chi_1 \cdots \chi_s = \chi_*^k$, gives

$$\begin{aligned} G(\overline{\chi}, p^m)\, \mathcal{J}_2 &= \sum_{x=1}^{p^m} \overline{\chi}(x) \sum_{x_1=1}^{p^m} \cdots \sum_{x_s=1}^{p^m} \chi_1(x_1) \cdots \chi_s(x_s) e_{p^m}\left(x \left(\sum_{i=1}^{s} x_i + B \prod_{i=1}^{s} x_i^{w_i} \right) \right) \\ &= \sum_{x=1}^{p^m} \sum_{x_1=1}^{p^m} \cdots \sum_{x_s=1}^{p^m} \overline{\chi\chi_1 \cdots \chi_s}(x) \chi_1(x_1) \cdots \chi_s(x_s) e_{p^m}\left(\sum_{i=1}^{s} x_i + B x^k \prod_{i=1}^{s} x_i^{w_i} \right) \\ &= \sum_{x=1}^{p^m} \sum_{x_1=1}^{p^m} \cdots \sum_{x_s=1}^{p^m} \overline{\chi}_*(x^k) e_{p^m}\left(B x^k \prod_{i=1}^{s} x_i^{w_i} \right) \prod_{i=1}^{s} \chi_i(x_i) e_{p^m}(x_i). \end{aligned}$$

Recall by Lemma 2.2.2 if $p \nmid x$, then the sum

$$\sum_{(\chi'')^k = \chi_0 \bmod p^m} \chi''(x) = \begin{cases} (k, \phi(p^m)), & \text{if } p \text{ is odd or } p^m = 2, 4, \\ 2(k, 2^{m-2}), & \text{if } p = 2,\ m \geq 3,\ k \text{ is even}, \\ 1, & \text{if } p = 2,\ m \geq 3,\ k \text{ is odd}, \end{cases} \tag{4.25}$$

if x is a kth power mod p^m, with the right-hand side equalling the number of times a kth power is achieved mod p^m, and equals zero otherwise. Thus we have

$$G(\overline{\chi}, p^m)\,\mathcal{J}_2 = \sum_{(\chi'')^k=\chi_0 \bmod p^m} \sum_{u=1}^{p^m} \sum_{x_1=1}^{p^m} \cdots \sum_{x_s=1}^{p^m} \overline{\chi''\chi_*}(u) e_{p^m}\left(p^n B_1 u \prod_{i=1}^{s} x_i^{w_i}\right) \prod_{i=1}^{s} \chi_i(x_i) e_{p^m}(x_i),$$

and substituting $u \mapsto u B_1^{-1} x_1^{-w_1} \cdots x_s^{-w_s}$ we have

$$G(\overline{\chi}, p^m)\mathcal{J}_2 = \sum_{(\chi'')^k=\chi_0 \bmod p^m} \chi''\chi_*(B_1) \sum_{u=1}^{p^m} \overline{\chi''\chi_*}(u) e_{p^m}(p^n u) \prod_{i=1}^{s} G(\chi_i(\chi''\chi_*)^{w_i}, p^m).$$

If $\chi''\chi_*$ is a primitive character mod p^{m-j} for some $j < n$, then by (4.24)

$$\sum_{u=1}^{p^m} \chi''\chi_*(u) e_{p^m}(p^n u) = p^j \sum_{u=1}^{p^{m-j}} \chi''\chi_*(u) e_{p^{m-j}}(p^{n-j} u) = 0. \tag{4.26}$$

Hence only if the character $\chi''\chi_*$ is a mod p^{m-n} character will (4.26) give a non-zero contribution, namely $p^n G(\overline{\chi''\chi_*}, p^{m-n})$, to the sum. In particular, we can restrict the sum to the mod p^{m-n} characters χ''.

Suppose that $m > n + t + \beta$. For p odd or $p = 2$ we (respectively) define c'' by

$$\chi''(a) = e_{\phi(p^{m-n})}(c'') \quad \text{or} \quad \chi''(5) = e_{2^{m-n-2}}(c''). \tag{4.27}$$

Since $(\chi'')^k = \chi_0 \bmod p^{m-n}$, we have $p^{m-n-t-\beta} | c''$. So χ'' and $(\chi'')^{w_i}$ are all mod $p^{t+\beta}$ characters with $t + \beta < m - n$.

Hence for all the χ'', we have that $\chi''\chi_*$ is primitive mod p^{m-n} iff χ_* is primitive mod p^{m-n} and $\chi_i(\chi''\chi_*)^{w_i}$ is primitive mod p^m iff $\chi_i\chi_*^{w_i}$ is primitive mod p^m. Observing that $G(\chi, p^j) = 0$ if χ is an imprimitive character mod p^j and $j \geq 2$, we deduce that $\mathcal{J}_2 = 0$ unless χ_* is primitive mod p^{m-n} and the $\chi_i\chi_*^{w_i}$ are primitive mod p^m.

□

For p odd and a primitive root a mod p^m, we define the integers R_j, $j \geq 1$, as

$$a^{\phi(p^j)} = 1 + R_j p^j. \tag{4.28}$$

Note that $R_j \equiv R_i \mod p^i$ for any $j \geq i$. For $p = 2$, we define R_j, $j \geq 2$, as

$$5^{2^{j-2}} = 1 + R_j 2^j, \tag{4.29}$$

with $R_j \equiv R_i \mod 2^{i-1}$ for $j \geq i$. We will need the following Gauss sum evaluation from [15].

Lemma 4.2.1. *Suppose that χ is a primitive character mod p^m with $m \geq 2$, then*

$$G(\chi, p^m) = p^{m/2}\chi(-cR_j^{-1})e_{p^m}(-cR_j^{-1}) \begin{cases} \left(\frac{-2rc}{p}\right)^m \varepsilon_{p^m}, & \text{if } p \neq 2, p^m \neq 27 \\ \left(\frac{2}{c}\right)^m \omega^c, & \text{if } p = 2 \text{ and } m \geq 5, \end{cases} \tag{4.30}$$

for any $j \geq \lceil \frac{m}{2} \rceil$ when p is odd and any $j \geq \lceil \frac{m}{2} \rceil + 2$ when $p = 2$ with $\omega = e^{\pi i/4}$, r, and ε_{p^m} as in (4.12) and (4.14). R_j is defined as in (4.28) or (4.29) with c as in (4.12) or (4.13).

When $p^m = 27$ an extra factor $e_3(-rc)$ is needed.

4.3 Proof of Theorem 4.0.1

Suppose that (4.15) holds. Since (4.23) plainly holds we can assume from Lemma 4.1.1 and Lemma 4.2.1 that $\chi\chi_1 \cdots \chi_s = \chi_*^k$ for some primitive mod p^{m-n} character χ_* with the $\chi_i\chi_*^{w_i}$ all primitive mod p^m (else the sum is zero). With β and c'' as in (4.15) and (4.27), we have $p^{m-n-t-\beta} \mid c''$ and χ'' is a mod $p^{t+\beta}$ character. In particular, since $m - n - t - \beta \geq t + \beta$, we have

$$\overline{\chi''}(c'' + c_*) = \overline{\chi''}(c_*). \tag{4.31}$$

Let l_1 be a positive integer with

$$l_1 \equiv c_*^{-1} c'' R_m^{-1} p^{-(m-n-t-\beta)} \bmod p^{t+\beta}.$$

Since $2(m-n-t-\beta) \geq m-n$ and, from the congruences after (4.28) and (4.29),

$$R_m \equiv R_{m-n-t-\beta} \mod p^{t+\beta},$$

we have

$$\begin{aligned} c'' + c_* &\equiv c_* \left(1 + l_1 R_m p^{m-n-t-\beta}\right) \bmod p^{m-n} \\ &\equiv c_* \left(1 + R_{m-n-t-\beta} p^{m-n-t-\beta}\right)^{l_1} \bmod p^{m-n} \\ &\equiv c_* \begin{cases} a^{l_1 \phi(p^{m-n-t-1})} \bmod p^{m-n}, & \text{for } p \text{ odd}, \\ 5^{l_1 2^{m-n-t-4}} \bmod 2^{m-n}, & \text{for } p = 2. \end{cases} \end{aligned}$$

Hence,

$$\overline{\chi_*}(c'' + c_*) = \overline{\chi_*}(c_*) e_{p^{t+\beta}}(-c_* l_1) = \overline{\chi_*}(c_*) e_{p^{m-n}}(-c'' R_m^{-1}),$$

and by (4.30) we have

$$G(\overline{\chi'' \chi_*}, p^{m-n}) = p^{\frac{m-n}{2}} \overline{\chi'' \chi_*}(c_* R_m^{-1}) e_{p^{m-n}}(c_* R_m^{-1}) \delta_a, \tag{4.32}$$

where, since $c'' + c_* \equiv c_* \bmod p$ for p odd, $c'' + c_* \equiv c_* \bmod 8$ for $p = 2$,

$$\delta_a = \begin{cases} \left(\frac{2rc_*}{p}\right)^{m-n} \varepsilon_{p^{m-n}}, & \text{for } p \text{ odd}, \ p^{m-n} \neq 3^3, \\ \left(\frac{2}{c_*}\right)^{m-n} \omega^{-c_*}, & \text{for } p = 2. \end{cases} \tag{4.33}$$

Similarly, since $2(m-t-\beta) \geq m$, we have

$$c_i + p^n w_i(c_* + c'') \equiv (c_i + p^n w_i c_*) \begin{cases} a^{l_2 \phi(p^{m-t-1})} \bmod p^m, & \text{for } p \text{ odd,} \\ 5^{l_2 2^{m-t-4}} \bmod 2^m, & \text{for } p = 2, \end{cases}$$

where l_2 is a positive integer with

$$l_2 \equiv (c_i + w_i p^n c_*)^{-1} w_i c'' p^{-(m-n-t-\beta)} R_m^{-1} \bmod p^{t+\beta}.$$

Note $(\chi'')^{w_i}(c_i + p^n w_i(c_* + c'')) = (\chi'')^{w_i}(c_i + p^n w_i c_*)$, and so

$$\begin{aligned} \chi_i(\chi''\chi_*)^{w_i}(c_i + w_i p^n(c_* + c'')) &= \chi_i(\chi''\chi_*)^{w_i}(c_i + w_i p^n c_*) e_{p^{t+\beta}}(l_2(c_i + w_i p^n c_*)) \\ &= \chi_i(\chi''\chi_*)^{w_i}(c_i + w_i p^n c_*) e_{p^{m-n}}(w_i c'' R_m^{-1}). \end{aligned}$$

Hence, using Lemma (4.2.1), we get

$$G(\chi_i(\chi''\chi_*)^{w_i}, p^m) = p^{\frac{m}{2}} \chi_i(\chi''\chi_*)^{w_i}(-(c_i + w_i p^n c_*) R_m^{-1}) e_{p^m}(-(c_i + w_i p^n c_*) R_m^{-1}) \delta_{b_i}, \quad (4.34)$$

where

$$\delta_{b_i} = \begin{cases} \left(\frac{-2r(c_i + w_i p^n c_*)}{p}\right)^m \varepsilon_{p^m}, & \text{for } p \text{ odd, } p^m \neq 3^3, \\ \left(\frac{2}{c_i + w_i 2^n c_*}\right)^m \omega^{c_i + w_i 2^n c_*}, & \text{for } p = 2. \end{cases} \quad (4.35)$$

For c defined as in (4.12) we have

$$\frac{1}{G(\overline{\chi}, p^m)} = p^{-\frac{m}{2}} \chi(c R_m^{-1}) e_{p^m}(-c R_m^{-1}) \delta_c, \quad (4.36)$$

where

$$\delta_c = \begin{cases} \left(\frac{2rc}{p}\right)^m \varepsilon_{p^m}^{-1}, & \text{for } p \text{ odd, } p^m \neq 3^3, \\ \left(\frac{2}{c}\right)^m \omega^c, & \text{for } p = 2. \end{cases} \tag{4.37}$$

Note, since $\chi\chi_1 \cdots \chi_s = \chi_*^k$ where $k = 1 - w_1 - \cdots - w_s$ and $(\chi'')^k = \chi_0$, we have

$$\overline{\chi''\chi_*}(-c_* R_m^{-1})\chi(-c_* R_m^{-1}) \prod_{i=1}^{s} \chi_i(\chi''\chi_*)^{w_i}(-c_* R_m^{-1}) = 1.$$

Since c is defined mod $\phi(p^m)$ we can replace c by $c = kp^n c_* - \sum_{i=1}^{s} c_i$, and then

$$e_{p^m}(p^n c_* R_m^{-1}) e_{p^m}(-c R_m^{-1}) \prod_{i=1}^{s} e_{p^m}(-(c_i + w_i p^n c_*) R_m^{-1}) = 1,$$

with $-c_* + \sum_{i=1}^{s}(c_i + w_i 2^n c_*) + c = (2^n - 1)c_*$ when $p = 2$. By substituting (4.32), (4.34), and (4.36) in (4.22) we get, for p^m and $p^{m-n} \neq 3^3$,

$$\begin{aligned} \mathcal{J}_2 &= p^{\frac{ms+n}{2}} \sum_{(\chi'')^k = \chi_0 \bmod p^{m-n}} \delta\, \chi''\chi_*(-B_1)\, \chi(-cc_*^{-1}) \prod_{i=1}^{s} \chi_i(\chi''\chi_*)^{w_i}(c_i c_*^{-1} + w_i p^n) \\ &= p^{\frac{ms+n}{2}} \delta\, \chi_*(\lambda)\chi(-cc_*^{-1}) \prod_{i=1}^{s} \chi_i(c_i c_*^{-1} + w_i p^n) \sum_{(\chi'')^k = \chi_0 \bmod p^{m-n}} \chi''(\lambda), \end{aligned}$$

with λ as in (4.14) and $\delta = \delta_a \delta_c \prod_{i=1}^{s} \delta_{b_i}$, with the product of the expressions in (4.33), (4.35), and (4.37) simplifying to the formula for δ given in (4.16) for p odd and (4.17) for $p = 2$. If λ is a kth power mod p^{m-n}, then (4.25) and $(k, \phi(p^{m-n})) = (k, p-1)p^t$ give

$$\mathcal{J}_2 = (k, p-1) p^{\frac{ms+n}{2} + \alpha} \delta \chi_*(\lambda)\chi(-cc_*^{-1}) \prod_{i=1}^{s} \chi_i(c_i c_*^{-1} + w_i p^n),$$

with α as in (4.18). If λ is not a kth power mod p^{m-n}, then

$$\sum_{(\chi'')^k=\chi_0 \bmod p^{m-n}} \chi''(\lambda) = 0$$

and $\mathcal{J}_2 = 0$. For $p^{m-n} = 3^3, n > 0$ we pick up an extra factor $e_3(rc_*)$ from $G(\overline{\chi''\chi_*}, p^{m-n})$. When $p^m = 3^3$ the additional factors in the Gauss sums cancel.

Bibliography

[1] B. Alsulmi, V. Pigno & C. Pinner, *Jacobi Type Sums with an Explicit Evaluation Modulo Prime Powers*, (https://www.math.ksu.edu/ $\sim$ pinner/research.html preprint 45.)

[2] B. Alsulmi, V. Pigno & C. Pinner, *Character Sums with an Explicit Evaluation*, to appear Math. Slovaca.

[3] T. Apostol, *Introduction to Analytic Number Theory*, Springer 1976.

[4] B. Berndt, R. Evans & K. Williams, *Gauss and Jacobi Sums*, Canadian Math. Soc. Series of Monographs and Advanced Texts, vol. 21, Wiley, New York 1998.

[5] T. Cochrane, *Exponential Sums Modulo Prime Powers*, Acta Arith. 101 (2002), no. 2, 131-149.

[6] T. Cochrane & Z. Zheng, *Pure and Mixed Exponential Sums*, Acta Arith. 91 (1999), no. 3, 249-278.

[7] T. Cochrane & Z. 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.

[8] G. Hardy & E. Wright, *An Introduction to the Theory of Numbers*, Oxford University Press, London 1979.

[9] K. Ireland & M. Rosen, *A Classical Introduction to Modern Number Theory*, Graduate Texts in Mathematics 84. Springer-Verlag, New York, 1990.

[10] C. Jacobi, *Brief an Gauss vom 8. Februar 1827*, Gesammelte Werke, vol. 7, pp. 393-400, Reimer, Berlin, 1891.

[11] R. Lidl & H. Niederreiter, *Finite Fields*, Encyclopedia of Mathematics and its Applications 20, 2nd edition, Cambridge University Press, 1997.

[12] J.-L. Mauclaire, *Sommes de Gauss modulo p^α, I & II*, Proc. Japan Acad. Ser. A 59 (1983), 109-112 & 161-163.

[13] I. Niven, H. Zuckerman & H. Montgomery, *An Introduction to the Theory of Numbers*, Fifth Edition, John Wiley and Sons, Inc, New York, 1991.

[14] R. Odoni, *On Gauss sums (mod p^n), $n \geq 2$*, Bull. London Math. Soc. 5 (1973), 325-327.

[15] M. Ostergaard, V. Pigno & C. Pinner, *Evaluating Prime Power Gauss and Jacobi Sums*, (http://www.math.ksu.edu/$\sim$ pinner/research.html preprint 44.)

[16] V. Pigno, *Prime Power Exponential and Character Sums with Explicit Evaluations*, Ph.D. Thesis, Kansas State University, 2014. (https://krex.k-state.edu).

[17] V. Pigno & C. Pinner, *Twisted Monomial Gauss Sums Modulo Prime Powers*, to appear Funct. Approx. Comment. Math. 51 (2014), no 2, 285-301.

[18] V. Pigno & C. Pinner, *Binomial Character Sums Modulo Prime Powers*, J. Théor. Nombres Bordeaux 28 (2016), 39-53.

[19] V. Pigno, C. Pinner & J. Sheppard, *Evaluating Binomial Character Sums Modulo Powers of Two*, J. Math. Res. Appl. 35 (2015), 137-142.

[20] J. Wang, *On the Jacobi sums mod P^n*, J. Number Theory 39 (1991), 50-64.

[21] J. Wang, *On the Jacobi Sums for Finite Commutative Rings with Identity*, J. Number Theory 48 (1994), 284-290.

[22] W. Zhang & T. Wang, *A Note on the Dirichlet Characters of Polynomials*, Math. Slovaca 64 (2014), no. 2, 301-310.

[23] W. Zhang & Z. Xu, *On the Dirichlet Characters of Polynomials of Several Variables*, Acta Arith. 121 (2006), no. 2, 117-124.

[24] W. Zhang & W. Yao, *A Note on the Dirichlet Characters of polynomials*, Acta Arith. 115 (2004), no. 3, 225-229.

[25] W. Zhang & Y. Yi, *On Dirichlet Characters of Polynomials*, Bull. London Math. Soc. 34 (2002), no. 4, 469-473.