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 $\chi_1, \chi_2$ 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 $\chi_1, \chi_2$ 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

$$J_1 = \sum_{x_1=1}^{p^m} \cdots \sum_{x_s=1}^{p^m} \chi_1(x_1) \cdots \chi_s(x_s),$$

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

$$J_2 = \sum_{x_1=1}^{p^m} \cdots \sum_{x_s=1}^{p^m} \chi_1(x_1) \cdots \chi_s(x_s)\chi(A_1 x_1 + \cdots + A_s x_s + B x_1^{w_1} \cdots x_s^{w_s}),$$

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 $\chi_1, \chi_2$ 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 $\chi_1, \chi_2$ 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

$$J_1 = \sum_{x_1=1}^{p^m} \cdots \sum_{x_s=1}^{p^m} \chi_1(x_1) \cdots \chi_s(x_s),$$

$$J_2 = \sum_{x_1=1}^{p^m} \cdots \sum_{x_s=1}^{p^m} \chi_1(x_1) \cdots \chi_s(x_s)\chi(A_1x_1 + \cdots + A_sx_s + Bx_1^{w_1} \cdots x_s^{w_s}),$$

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

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.
# Table of Contents

Table of Contents

List of Tables

Acknowledgements

Dedication

1 Introduction

2 Preliminaries
   2.1 Dirichlet Characters
   2.2 Gauss Sums
   2.3 Jacobi Sums
   2.4 Generalized Jacobi Sums

3 Evaluating Jacobi Type Sums Modulo Prime Powers
   3.1 Writing $J_1$ in Terms of Gauss Sums
   3.2 Proof of Theorem 3.0.2
   3.3 The Case $p = 2$
   3.4 Imprimitive Characters

4 Character Sums with an Explicit Evaluation
   4.1 Preliminaries
   4.2 Writing $J_2$ in Terms of Gauss Sums
4.3 Proof of Theorem 4.0.1 ............................................. 53

Bibliography .......................................................... 58
List of Tables

2.1 $q = 3, \phi(q) = 2$ .................................................. 9
2.2 $q = 4, \phi(q) = 2$ .................................................. 9
2.3 $q = 5, \phi(q) = 4$ .................................................. 9
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 $\chi$ the classical Gauss sums

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

where $e_k(x) := e^{2\pi ix/k}$, 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 $\chi_1, \chi_2 \text{ mod } p$ 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 \( \chi_1, \chi_2 \) 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 \( \chi_1, \ldots, \chi_s \) are mod \( p \) characters, we can define
\[
J(\chi_1, \ldots, \chi_s, p) := \sum_{x_1=1}^{p} \cdots \sum_{x_s=1}^{p} \chi_1(x_1) \cdots \chi_s(x_s). \quad (1.1)
\]
If \( \chi_1 \cdots \chi_s \) is non-trivial, then we can write (1.1) in the form
\[
J(\chi_1, \ldots, \chi_s, p) = \frac{\prod_{i=1}^{s} G(\chi_i, p)}{G(\chi_1 \cdots \chi_s, p)},
\]
and if \( \chi_1, \ldots, \chi_s, \chi_1 \cdots \chi_s \) are non-trivial characters, then
\[
|J(\chi_1, \ldots, \chi_s, p)| = p^{\frac{s-1}{2}}.
\]

Here we are interested in working in the ring \( \mathbb{Z}_{p^m} \) rather than the finite field \( \mathbb{F}_{p^m} \). When \( \chi_1, \ldots, \chi_s \), are mod \( p^m \) Dirichlet characters one can similarly define the Jacobi sums
\[
J(\chi_1, \ldots, \chi_s, p^m) := \sum_{x_1=1}^{p^m} \cdots \sum_{x_s=1}^{p^m} \chi_1(x_1) \cdots \chi_s(x_s). \quad (1.2)
\]
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

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

(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 $x_1^p + \cdots + x_s^p \equiv 1 \mod p^2$ 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

$$J_B(\chi_1, \ldots, \chi_s, p^m) := \sum_{x_1=1}^{p^m} \cdots \sum_{x_s=1}^{p^m} \chi_1(x_1) \cdots \chi_s(x_s),$$

(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

\[
\mathcal{J}_1 := \sum_{x_1=1}^{p^m} \cdots \sum_{x_s=1}^{p^m} \chi_1(x_1) \cdots \chi_s(x_s), \tag{1.5}
\]

where

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

and

\[
\mathcal{J}_2 := \sum_{x_1=1}^{p^m} \cdots \sum_{x_s=1}^{p^m} \chi_1(x_1) \cdots \chi_s(x_s) \chi(A_1 x_1 + \cdots + A_s x_s + B x_1^{w_1} \cdots x_s^{w_s}), \tag{1.7}
\]

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 \( \chi'_i \mod p^m \) such that \( \chi'_1 \cdots \chi'_s \) is a primitive \( \mod p^m \) character, and for all \( i \), the \( A_i^{-1} B c'_i v'^{-1} \equiv \alpha_i^{k_i} \mod p^m \) for some \( \alpha_i \), 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

\[ |J_1| = (k_1, p - 1) \cdots (k_s, p - 1)p^{m_2(s-1)}. \]

Otherwise \( J_1 = 0. \)

The following evaluation of \( J_2 \) is a special case of Theorem 4.0.1 which we shall prove in Chapter 4. Again we have stated the theorem here for \( |J_2| \), but in Theorem 4.0.1 in Chapter 4 we obtain an evaluation for \( J_2 \) without assuming that condition (1.8) holds. The corresponding \( p = 2 \) result is given in Theorem 4.0.1 for \( J_2 \).

**Theorem 1.0.2.** Let \( p \) be an odd prime and \( \chi, \chi_1, \ldots, \chi_s \) be mod \( p^m \) characters with \( \chi \) 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 \( \chi^* \) such that the \( \chi_i \chi^*_i \) are all primitive characters mod \( p^m \), and \( \lambda \) defined as:

\[
\lambda := -B \prod_{i=1}^{s} (c_i c_i^{-1} + w_i)^{w_i} \mod p^m
\]

is a \( k \)th power mod \( p^m \), then

\[ |J_2| = (k, p - 1)p^{m_2} \]

where for a primitive root \( a \), \( c_i \) and \( c_i^* \) are defined as

\[
\chi_i(a) = e_{\phi(p^m)}(c_i), \quad \chi^*(a) = e_{\phi(p^m-n)}(c^*_i).
\]

Otherwise \( J_2 = 0. \)

Both sums \( J_1 \) and \( J_2 \) 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 \( J_1 \) and \( J_2 \), 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 $\chi$ 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 $\chi$ 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 $\hat{G}$. Note $\hat{G}$ form a group. For any two characters $\chi_1, \chi_2$ in $\hat{G}$, 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 $\chi_0$, the principal character. The inverse of a character $\chi$ is its complex conjugate defined by $\chi^{-1}(x) = \overline{\chi(x)}$. If $\chi \in \hat{G}$, then $\chi^{-1} \in \hat{G}$. $\hat{G}$ 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 $\chi$ is defined by
\( \chi(a_j) \) where the \( \chi(a_j) \) are \( n_j \)th roots of unity. Thus we have \( n_j \) choices for \( \chi(a_j) \) and have \( n_1 \cdots n_k \) choices for \( \chi \). So \( |\hat{G}| = n_1 \cdots n_k = |G| \). In fact, it is easy to see that \( \hat{G} \) is generated by \( \chi_1, \ldots, \chi_k \) where \( \chi_l(a_i) = e^{2\pi i / n_l} \) and \( \chi_l(a_j) = 1 \) for all \( j \neq l \) so that \( G \cong \hat{G} \). 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. \( \chi \) is completely multiplicative, that is \( \chi(ab) = \chi(a)\chi(b) \) for all \( a, b \in \mathbb{Z} \),
3. \( \chi \) 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 \( \chi_0 \) (mod \( q \)) is the character with

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

**Example**

When \( q = 1 \) or \( q = 2 \), then \( \phi(q) = 1 \) and the principal character \( \chi_0 \) 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.

<p>| Table 2.1: ( q = 3, \phi(q) = 2 ) | Table 2.2: ( q = 4, \phi(q) = 2 ) |</p>
<table>
<thead>
<tr>
<th>n</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>n</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \chi_1(n) )</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>( \chi_1(n) )</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>( \chi_2(n) )</td>
<td>1</td>
<td>-1</td>
<td>0</td>
<td>( \chi_2(n) )</td>
<td>1</td>
<td>0</td>
<td>-1</td>
<td>0</td>
</tr>
</tbody>
</table>

<p>| Table 2.3: ( q = 5, \phi(q) = 4 ) |</p>
<table>
<thead>
<tr>
<th>n</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \chi_1(n) )</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>( \chi_2(n) )</td>
<td>1</td>
<td>-1</td>
<td>-1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>( \chi_3(n) )</td>
<td>1</td>
<td>( i )</td>
<td>( -i )</td>
<td>-1</td>
<td>0</td>
</tr>
<tr>
<td>( \chi_4(n) )</td>
<td>1</td>
<td>( -i )</td>
<td>( i )</td>
<td>-1</td>
<td>0</td>
</tr>
</tbody>
</table>

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

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

(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 $\left( \frac{a^2b}{p} \right) = \left( \frac{b}{p} \right)$.
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 \pmod{4}, \\
-1, & \text{if } p \equiv 3 \pmod{4}.
\end{cases}
6. $\left( \frac{2}{p} \right) = (-1)^{(p^2-1)/8} = \begin{cases} 
1, & \text{if } p \equiv 1 \text{ or } 7 \pmod{8}, \\
-1, & \text{if } p \equiv 3 \text{ or } 5 \pmod{8}.
\end{cases}$
7. Gaussian reciprocity law: If $p$ and $q$ are distinct odd primes, then

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

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

Induced Modulus

Let $\chi$ be a Dirichlet character mod $q$. For $q_1 | q$ we say that $\chi$ is an induced by a mod $q_1$ character, $\chi_{q_1}$, 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 $\chi$ if we have

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

Note that for any Dirichlet character $\chi$ 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 \( \chi_0 \) 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 \( \chi \) is a nonprincipal character mod \( p \), where \( p \) is a prime, then \( \chi \) 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 \( \chi \) 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 \( a^{\phi(q)} \equiv 1 \mod q \). In this thesis we are concerned with the case where \( \chi \) 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 \( \chi_1(\mod p_1^{\alpha_1}), \chi_2(\mod p_2^{\alpha_2}), \ldots, \chi_k(\mod p_k^{\alpha_k}) \). Then, we can construct a mod \( q \) character \( \chi \) 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

\[
\chi(m) = \chi_1(a)\chi_2(1) \cdots \chi_k(1) = \chi_1(a), \quad \text{and} \quad \chi'(m) = \chi'_1(a)\chi'_2(1) \cdots \chi'_k(1) = \chi'_1(a).
\]

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 $\varphi$ on prime powers $p^\alpha$ is

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

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

**Lemma 2.1.1.** Let $\chi$ be a Dirichlet character mod $q$. Then,

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

**Proof.** Let

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

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

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

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

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

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

$$S = \sum_{a \mod q} \chi_0(a) = \phi(q).$$
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 \( \chi_i \mod q \), then for \( g \in \mathbb{Z}[x_1, \ldots, x_s] \), define the more general sum

\[
S(\vec{\chi}, \vec{f}, q) := \sum_{x_1=1}^{q} \cdots \sum_{x_s=1}^{q} g(x_1, \ldots, x_s) \equiv 0 \mod q
\]

\[
\chi_1(f_1(x_1, \ldots, x_s)) \cdots \chi_k(f_k(x_1, \ldots, x_s)).
\]  

(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 \( \chi'_i \) and \( \chi''_i \) 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 \( \chi_i \) is a mod \( uv \) character with \( (u, v) = 1 \), and \( \chi_i = \chi'_i\chi''_i \), where \( \chi'_i \) is a mod \( u \) and \( \chi''_i \) is a mod \( v \) character. Write \( x_i = e_iuv^{-1} + t_iuu^{-1} \), where \( uu^{-1} + vv^{-1} = 1 \) and \( e_i = 1, \ldots, u, t_i = 1, \ldots, v \). Note

\[
\chi_i(f_i(x_1, \ldots, x_s)) = \chi'_i\chi''_i(f_i(e_1uv^{-1} + t_1uu^{-1}, \ldots, e_suv^{-1} + t_suu^{-1}))
\]

\[
= \chi'_i(f_i(e_1, \ldots, e_s))\chi''_i(f_i(t_1, \ldots, t_s)).
\]

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

\[
g(x_1, \ldots, x_s) \equiv 0 \mod uv \iff \begin{cases} 
  g(x_1, \ldots, x_s) \equiv 0 \mod u, \\
  g(x_1, \ldots, x_s) \equiv 0 \mod v,
\end{cases}
\]

\[
\iff \begin{cases} 
  g(e_1, \ldots, e_s) \equiv 0 \mod u, \\
  g(t_1, \ldots, t_s) \equiv 0 \mod v.
\end{cases}
\]
Writing $S := S(\vec{\chi}, \vec{f}, uv)$, then we have

$$S = \sum_{e_1=1}^u \sum_{t_1=1}^v \cdots \sum_{e_s=1}^u \sum_{t_s=1}^v \chi_1(f_1(e_1, \ldots, e_s))\chi'_1(f_1(t_1, \ldots, t_s)) \cdots \chi'_k(f_k(e_1, \ldots, e_s))\chi''_k(f_k(t_1, \ldots, t_s))$$

$$g(e_1, \ldots, e_s) \equiv 0 \mod u$$

$$g(t_1, \ldots, t_s) \equiv 0 \mod v$$

$$= \sum_{e_1=1}^u \cdots \sum_{e_s=1}^u \chi'_1(f_1(e_1, \ldots, e_s)) \cdots \chi'_k(f_k(e_1, \ldots, e_s))$$

$$\times \sum_{t_1=1}^v \cdots \sum_{t_s=1}^v \chi''_1(f_1(t_1, \ldots, t_s)) \cdots \chi''_k(f_k(t_1, \ldots, t_s))$$

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

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 $\chi$ we define the Gauss sum by

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

where we recall that $e_k(x) = e^{2\pi i x/k}$. 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 $\chi$ is the Legendre symbol, $G(\chi, p)$ is called a quadratic Gauss sum, and will be denoted simply as $G_p$. We would like to start with the following Lemma in order to understand the Gauss sums properties.
Lemma 2.2.1.

\[
\sum_{x=0}^{q-1} e_q(Ax) = \begin{cases} 
q, & \text{if } A \equiv 0 \mod q, \\
0, & \text{else.}
\end{cases}
\]  

(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

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

\[\square\]

More generally we can define

\[\mathcal{S}(A, \chi) := \sum_{x=1}^{q} \chi(x)e_q(Ax).\]  

(2.8)

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

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

Proof. Suppose \( \mathcal{S}(A, \chi) \neq 0 \) for some \( (A, q) > 1 \), then we need to show \( \chi \) is imprimitive.

Take \( q_1 := q/(A, q) \) and suppose that \( m \equiv 1 \mod q_1 \) with \( (m, q) = 1 \). Note

\[
e_q(Ajm) = e^{\frac{2\pi i Ajm}{q}} = e^{\frac{2\pi i Ajm}{q_1(A,q)}},
\]

\[
= e_{q_1} \left( \frac{Ajm}{(A, q)} \right) = e_{q_1} \left( \frac{A}{(A, q)} \right)
\]

\[
= e^{\frac{2\pi i Aj}{q_1(A,q)}} = e^{\frac{2\pi i Aj}{q}}
\]

\[
= e_q(Aj).
\]
Thus we have

\[ \mathcal{G}(A, \chi) = \sum_{j \mod q} \chi(j)e_q(Aj) \]

\[ = \sum_{j \mod q} \chi(jm)e_q(Ajm) \quad j := jm \]

\[ = \chi(m) \sum_{j=1}^{q} \chi(j)e_q(Aj) \]

\[ = \chi(m) \mathcal{G}(A, \chi). \]

Since \( \mathcal{G}(A, \chi) \neq 0 \) we must have \( \chi(m) = 1 \) which shows that \( \chi \) is induced by a mod \( q \) character. Thus \( \chi \) is imprimitive.

\[ \square \]

**Proposition 2.2.1.** If \( \chi \) is any Dirichlet character mod \( q \), then

\[ \mathcal{G}(A, \chi) = \overline{\chi(A)} \mathcal{G}(1, \chi) \quad \text{whenever} \ (A, q) = 1. \]

**Proof.** Let \( \mathcal{G}(A, \chi) = \sum_{x=1}^{q} \chi(x)e_q(Ax). \) 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:

\[
\mathfrak{S}(A, \chi) = \sum_{x=1}^{q} \chi(x)e_q(Ax)
\]

\[
= \chi(A) \sum_{x=1}^{q} \chi(Ax)e_q(Ax)
\]

\[
= \chi(A) \sum_{y=1}^{q} \chi(y)e_q(y), \quad y := Ax
\]

\[
= \chi(A) \mathfrak{S}(1, \chi).
\]

\[\Box\]

**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 \( \chi \) 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 \( \chi \) 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 \( \mathfrak{S}(A, \chi) = \chi(A)\mathfrak{S}(1, \chi) \), and so

\[
|\mathfrak{S}(A, \chi)|^2 = \mathfrak{S}(A, \chi)\mathfrak{S}(A, \chi)
\]

\[
= \left( \chi(A)\mathfrak{S}(1, \chi) \right) \left( \chi(A)\mathfrak{S}(1, \chi) \right)
\]

\[
= |\mathfrak{S}(1, \chi)|^2.
\]
Furthermore

\[ |\mathcal{S}(1, \chi)|^2 = \sum_{j \mod q} \chi(j)e_q(j) \sum_{k \mod q} \overline{\chi(k)}e_q(-k) \]

\[ = \sum_{(k,q)=1} \overline{\chi(k)} \left( \sum_{j} \chi(j)e_q(j) \right)e_q(-k) \]

\[ = \sum_{(k,q)=1} \overline{\chi(k)} \left( \sum_{j} \chi(jk)e_q(jk) \right)e_q(-k), \quad j := jk \]

\[ = \sum_{(k,q)=1} e_q(-k) \left( \sum_{j} \chi(j)e_q(jk) \right). \]

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

\[ |\mathcal{S}(1, \chi)|^2 = \sum_{k=1}^{q} \sum_{j=1}^{q} \chi(j)e_q(k(j - 1)) \]

\[ = \sum_{j=1}^{q} \chi(j) \left( \sum_{k=1}^{q} e_q(k(j - 1)) \right). \]

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 \( |\mathcal{S}(1, \chi)|^2 = q\chi(1) = q. \)

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 $k$th power mod $p^m$, then

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

(2.9)

If $u$ is not a $k$th power mod $p^m$, then

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

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 $\chi$ 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 $c = \phi(p^m)/D$ 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 $k$th power mod $p^m$, then

$$
\sum_{\chi^D = \chi_0} \chi(u) = D.
$$
If $u$ is not a $k$th power mod $p^m$, then $u = a^\gamma$ where $\gamma \not\equiv k\gamma' \mod \phi(p^m)$ for some $\gamma'$ 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 $\mathbb{Z}^*_2$ (see [13]). Define $\chi(-1) = e_{2}(c_0), \ 1 \leq c_0 \leq 2,$ and $\chi(5) = e_{2m-2}(c), \ 1 \leq c \leq 2^{m-2}$.

If $\chi^k = \chi_0$, then we have the congruences $kc \equiv 0 \mod 2^{m-2}$ and $kc_0 \equiv 0 \mod 2$ 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 $k$th power mod $2^m$, then

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

If $k$ is odd then every odd $u$ is a $k$th power. If $u$ is not a $k$th 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 $\chi_0$ and $u^k \equiv u \mod 2$

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

If $p = 4$, then as seen in Table 2.2 we have two characters $\chi_1, \chi_2$ where

$$\chi_1(u) = \begin{cases} 0, & \text{if } u \text{ is even,} \\ 1, & \text{if } u \text{ is odd,} \end{cases}$$

and

$$\chi_2(u) = \begin{cases} 1, & \text{if } u \equiv 1 \mod 4, \\ -1, & \text{if } u \equiv 3 \mod 4, \\ 0, & \text{if } u \equiv 0 \mod 4. \end{cases}$$

Thus, we get

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

Recall that $G_p$ is the quadratic Gauss sum,

$$G_p := \sum_{x=1}^{p-1} \left( \frac{x}{p} \right) e_p(x).$$  \hspace{1cm} (2.10)

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

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

$$G_p := \sum_{x=0}^{p-1} e_p(x^2) = \begin{cases} \pm \sqrt{p}, & \text{if } p \equiv 1 \mod 4, \\ \pm i \sqrt{p}, & \text{if } p \equiv 3 \mod 4. \end{cases}$$  \hspace{1cm} (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]),

\[ G_p = \begin{cases} 
\sqrt{p}, & \text{if } p \equiv 1 \mod 4, \\
\iota \sqrt{p}, & \text{if } p \equiv 3 \mod 4.
\end{cases} \]

From the definition of the quadratic Gauss sum, we have

\[
G_p^2 = \sum_{x=1}^{p-1} \left( \frac{x}{p} \right) e_p(x) \sum_{y=1}^{p-1} \left( \frac{y}{p} \right) e_p(y) \\
= \sum_{x=1}^{p-1} \left( \frac{x}{p} \right) e_p(x) \left( \sum_{y=1}^{p-1} \left( \frac{xy}{p} \right) e_p(xy) \right) \\
= \sum_{y=1}^{p-1} \left( \frac{y}{p} \right) \sum_{x=1}^{p-1} e_p(x(y + 1)).
\]

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

\[
G_p^2 = (-1) \sum_{y=1}^{p-2} \left( \frac{y}{p} \right) + \left( \frac{-1}{p} \right) (p - 1) \\
= (-1) \sum_{y=1}^{p-1} \left( \frac{y}{p} \right) + \left( \frac{-1}{p} \right) + \left( \frac{-1}{p} \right) (p - 1) = \left( \frac{-1}{p} \right) p.
\]

From the property (5) in Lemma 2.1.1 we get the desired result. \( \square \)
2.3 Jacobi Sums

Definition 2.3.1. For two Dirichlet characters \( \chi_1, \chi_2 \mod q \), we define the classical Jacobi sums as

\[
J(\chi_1, \chi_2, q) := \sum_{x=1}^{q} \chi_1(x) \chi_2(1 - x).
\] (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 \( \chi_1 \) and \( \chi_2 \) be characters on \( \mathbb{Z}_p \), where \( p \) is a prime.

(a) If \( \chi_1 \) and \( \chi_2 \) are both principal characters, then \( J(\chi_1, \chi_2, p) = p - 2 \).

(b) If one of \( \chi_1 \) and \( \chi_2 \) is principal, then \( J(\chi_1, \chi_2, p) = -1 \).

(c) If \( \chi \) is nonprincipal, then \( J(\chi, \chi, p) = -\chi(-1) \).

Proof. (a) Since both \( \chi_1 \) and \( \chi_2 \) 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 \( \chi_1 \) is principal and \( \chi_2 \) 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 \( \chi \) is nonprincipal, then

\[
J(\chi, \chi, p) = \sum_{x \in \mathbb{Z}_p^*} \chi(x^{-1}) \chi(1 - x) = \sum_{x \in \mathbb{Z}_p^*} \chi(x^{-1} - 1)
\]

\[
= \sum_{x \in \mathbb{Z}_p^*} \chi(x - 1) = \sum_{x \in \mathbb{Z}_p} \chi(x - 1) - \chi(-1) = -\chi(-1).
\]

\[\qed\]

The following theorem shows that the mod \( q \) Jacobi sums (2.12) can be written in terms
Lemma 2.3.1. If \( \chi_1, \chi_2 \) are characters mod \( q \) such that \( \chi_1 \chi_2 \) is primitive, then for any \( z \in \mathbb{Z} \)
\[
\sum \sum_{x_1 + x_2 \equiv z \mod q} \chi_1(x_1) \chi_2(x_2) = \chi_1 \chi_2(z) J(\chi_1, \chi_2, q).
\]
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 \( \chi_1, \chi_2 \) 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
\[
\sum \sum_{x_1 + x_2 \equiv z \mod q} \chi_1(x_1) \chi_2(x_2) = \chi_1 \chi_2(z) \sum \sum_{x_1 + x_2 \equiv 1 \mod q} \chi_1(x_1) \chi_2(x_2)
\]
\[
= \chi_1 \chi_2(z) J(\chi_1, \chi_2, q).
\]

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
\[
\sum \sum_{x_1 + x_2 \equiv z \mod q} \chi_1(x_1) \chi_2(x_2) = \chi_1 \chi_2(u) \sum \sum_{x_1 + x_2 \equiv z \mod q} \chi_1(x_1) \chi_2(x_2).
\]
Hence
\[
\sum \sum_{x_1 + x_2 \equiv z \mod q} \chi_1(x_1) \chi_2(x_2) = 0.
\]

\( \square \)

Theorem 2.3.2. Let \( \chi_1 \) and \( \chi_2 \) 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 \( \chi_1, \chi_2, \) 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

\[
G(\chi_1, q)G(\chi_2, q) = \sum_x \sum_y \chi_1(x)\chi_2(y)e_q(x + y) \\
= \sum_z e_q(z) \sum_{x+y=z} \chi_1(x)\chi_2(y) \\
= J(\chi_1, \chi_2, q) \sum_z \chi_1\chi_2(z)e_q(z) \\
= J(\chi_1, \chi_2, q)G(\chi_1\chi_2, q).
\]

Now suppose that \( \chi_1, \chi_2, \) and \( \chi_1\chi_2 \) are all primitive. Then from Proposition 2.2.2, we get

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

\[ \square \]

### 2.4 Generalized Jacobi Sums

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

\[
J(\chi_1, \ldots, \chi_s, q) := \sum_{x_1+\cdots+x_s \equiv 1 \text{ mod } q} \chi_1(x_1)\cdots\chi_s(x_s), \tag{2.13}
\]

where the summation is taken over all \( q^{s-1} \) \( s \)-tuples \( (x_1, \ldots, x_s) \) 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
\[
J_B(\chi_1, \ldots, \chi_s, p^m) := \sum_{x_1=1}^{p^m} \cdots \sum_{x_s=1}^{p^m} \chi_1(x_1) \cdots \chi_s(x_s). \tag{2.14}
\]

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
\[
J_B(\chi_1, \ldots, \chi_s, p^m) = \sum_{x_1=1}^{p^m} \cdots \sum_{x_s=1}^{p^m} \chi_1(x_1 B') \cdots \chi_s(x_s B')
\]
\[
= (\chi_1 \cdots \chi_s)(B') \sum_{x_1=1}^{p^m} \cdots \sum_{x_s=1}^{p^m} \chi_1(x_1) \cdots \chi_s(x_s)
\]
\[
= (\chi_1 \cdots \chi_s)(B') J_{p^n}(\chi_1, \ldots, \chi_s, p^m). \tag{2.15}
\]

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 \( \chi_0 \) is the principal character.
Proof. In the sums below, the $x_i$ run through complete residue systems mod $p^m$. 

$$J_0(\chi_1, \ldots, \chi_s, p^m) = \sum_{x_1 + \cdots + x_s = 0} \chi_1(x_1) \cdots \chi_s(x_s)$$

$$= \sum_{x_s} \left( \sum_{x_1 + \cdots + x_{s-1} = -x_s} \chi_1(x_1) \cdots \chi_{s-1}(x_{s-1}) \right) \chi_s(x_s)$$

$$= \sum_{(x_s, p) = 1} \left( \sum_{x_1 + \cdots + x_{s-1} = -x_s} \chi_1(x_1) \cdots \chi_{s-1}(x_{s-1}) \right) \chi_s(x_s)$$

$$= \sum_{(x_s, p) = 1} ((\chi_1 \cdots \chi_{s-1})(-x_s)J(\chi_1, \ldots, \chi_{s-1}, p^m)) \chi_s(x_s), \quad x_i \mapsto -x_i x_s$$

$$= \chi_s(-1)J(\chi_1, \ldots, \chi_{s-1}, p^m) \sum_{x_s} (\chi_1 \cdots \chi_s)(-x_s)$$

$$= \chi_s(-1)J(\chi_1, \ldots, \chi_{s-1}, p^m) \sum_{x_s} (\chi_1 \cdots \chi_s)(x_s).$$

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 \( \chi_1, \chi_2 \mod q \) the classical Jacobi sum is

\[
J(\chi_1, \chi_2, q) := \sum_{x=1}^{q} \chi_1(x)\chi_2(1-x).
\]  
(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

\[
J_B(\chi_1, \ldots, \chi_s, q) := \sum_{x_1=1}^{q} \cdots \sum_{x_s=1}^{q} \chi_1(x_1) \cdots \chi_s(x_s) \quad \text{if} \quad x_1 + \cdots + x_s \equiv B \mod q.
\]  
(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 $\chi_i \mod q$. Then for an $h \in \mathbb{Z}[x_1, \ldots, x_s]$ and $B \in \mathbb{Z}$ we can define

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

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

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

where the $k_i$ are non-zero integers, and

$$J_1 := J_B(\vec{\chi}, h_1, p^m) = \sum_{x_1=1}^{p^m} \cdots \sum_{x_s=1}^{p^m} (A_1 x_1^{k_1} + \cdots + A_s x_s^{k_s} \equiv B \mod p^m) \chi_1(x_1) \cdots \chi_s(x_s). \quad (3.5)$$

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

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

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 $B$

$$B = p^n B', \quad p \nmid B'. \quad (3.7)$$
The evaluation in [15] relied on expressing (3.2) in terms of Gauss sums
\[ G(\chi, p^m) := \sum_{x=1}^{p^m} \chi(x) e_{p^m}(x), \] (3.8)
where \( e_k(x) = e^{2\pi ix/k} \). For example, if at least one of the \( \chi_i \) is primitive mod \( p^m \) and \( m > n \) then \( J_B(\chi_1, \ldots, \chi_s, p^m) = 0 \) unless \( \chi_1 \cdots \chi_s \) is a mod \( p^{m-n} \) character, in which case
\[ J_B(\chi_1, \ldots, \chi_s, p^m) = \chi_1 \cdots \chi_s(B') p^{-(m-n)} \frac{G(\chi_1 \cdots \chi_s, p^{m-n}) \prod_{i=1}^{s} G(\chi_i, p^m)}{G(\chi_1, \ldots, \chi_s, p^m)^s}, \] (3.9)
(see for example [15, Theorem 2.2]). In particular if \( m \geq n + 2 \) and at least one of the \( \chi_i \) is primitive we see that \( J_B(\chi_1, \ldots, \chi_s, p^m) = 0 \) unless all the \( \chi_i \) 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):
\[ J_B(\chi_1, \ldots, \chi_s, p^m) = p^{\frac{1}{2}(m(s-1)+n)} \frac{\chi_1(B'c_1) \cdots \chi_s(B'c_s)}{\chi_1 \cdots \chi_s(v)} \delta(\chi_1, \ldots, \chi_s), \] (3.10)
where, when \( p \) is odd,
\[ \delta(\chi_1, \ldots, \chi_s) = \left( \frac{-2r}{p} \right)^{m(s-1)+n} \left( \frac{v}{p} \right)^{m-n} \left( \frac{c_1 \cdots c_s}{p} \right)^m \varepsilon_{p^m}^{-1} \varepsilon_{p^{m-n}}^{-1}, \] (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
\[ a^{\phi(p)} = 1 + rp, \quad \chi_i(a) = e_{\phi(p^m)}(c_i), \quad 1 \leq c_i \leq \phi(p^m). \] (3.12)
Here, as usual, $\left( \frac{x}{y} \right)$ denotes the Jacobi symbol,

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

(3.13)

and

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

(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

$$
p^{t_i} \parallel k_i, \quad t := \max\{t_1, \ldots, t_s\}.
$$

(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 $x_i^{k_i} \equiv x_i^{k_i/p} \pmod{p^m}$ and one can replace $k_i$ by $k_i/p$. We define $d_i$ and $D_i$ by

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

(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 $\chi'_1 \cdots \chi'_s$ mod $p^m$ such that $\chi'_1 \cdots \chi'_s$ is induced
by a primitive mod $p^{m-n}$ character, and the $A_i^{-1}B'_i c'_i v'-1 \equiv \alpha_i^{k_i}$ mod $p^m$ for some $\alpha_i$, then

$$J_1 = D_1 \cdots D_s p^{2(m(s-1)+n)} \chi_1(\alpha_1) \cdots \chi_s(\alpha_s) \delta(\chi'_1, \ldots, \chi'_s),$$

(3.17)

where the $c'_i$ define the $\chi'_i$ 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 $J_1 = 0$.

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

We prove the theorem in Section 3.2, but first we show that the $\chi_i$ must be $k_i$th powers and express $J_1$ in terms Jacobi sums (3.2) and hence in terms of Gauss sums.

### 3.1 Writing $J_1$ in Terms of Gauss Sums

We first show that $J_1 = 0$ unless each $\chi_i$ is a $k_i$th 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

$$J = \sum_{x_1=1}^{p^m} \cdots \sum_{x_s=1}^{p^m} \chi_1(x_1) \cdots \chi_s(x_s) \chi(f(x_1^{k_1}, \ldots, x_s^{k_s})) c_p^m(g(x_1^{k_1}, \ldots, x_s^{k_s})),$$

$$h(x_1^{k_1}, \ldots, x_s^{k_s}) \equiv B \text{ mod } p^m$$

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

32
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

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

$$= \chi_1(z_1) J.$$ 

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 $1 = \chi_1(z_1) = \chi_1(a)^\phi(p^m)/(k_1 \phi(p^m)) = e^{2\pi ic_1/(k_1 \phi(p^m))}$ and $(k_1, \phi(p^m)) | c_1$. Hence there is an integer $c_1'$ satisfying

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

and $\chi_1 = (\chi_1')^{k_1}$ where $\chi_1'$ 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 $(k_1, 2^{m-2}) | c_1$ and there exists a $c_1'$ with $c_1' k_1 \equiv c_1 \mod 2^{m-2}$. 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 $\chi_i$ are $k_i$th 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 $\chi_i$, $1 \leq i \leq s$, $h_1$ be of the form (3.4). Then,

$$J_1 = \sum_{\substack{(\chi''_i)^{k_i} = \chi_0 \atop i = 1, \ldots, s}} \left( \prod_{j=1}^{s} \chi_j' \chi''_j (A_j^{-1}) \right) J_B (\chi_1', \ldots, \chi_s', \chi''_1, p^m),$$

where $\chi_0$ 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

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

and at least one of the characters is primitive mod $p^m$ then $J_1 = 0$ unless all the $\chi_i'$ are primitive mod $p^m$ with $\chi_1' \cdots \chi_s'$ induced by a primitive mod $p^{m-n}$ character, in which case

$$J_1 = \sum_{\substack{(\chi''_i)^{k_i} = \chi_0 \atop i = 1, \ldots, s}} \frac{\prod_{i=1}^{s} \chi'_i \chi''_i (A_i^{-1}B') G(\chi'_i, \chi''_i, p^m)}{G(\chi_1'' \cdots \chi''_s, p^{m-n})}.$$  \hfill (3.19)

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

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

if $u$ is a $k_i$th power mod $p^m$ (where each $k_i$th power is achieved $D_i$ times) and equals zero otherwise.
Making the substitution $u_i \mapsto A_i^{-1}u_i$, we have

$$J_1 = \sum_{x_1=1}^{p^m} \cdots \sum_{x_s=1}^{p^m} \chi_1(x_1^{k_1}) \cdots \chi_s(x_s^{k_s})$$

$$= \sum_{(\chi''_i)_{i=1,\ldots,s} = \chi_0}^{(\chi''_i)_{i=1,\ldots,s} = \chi_0} \sum_{u_1=1}^{p^m} \cdots \sum_{u_s=1}^{p^m} \chi'_1(u_1) \cdots \chi'_s(u_s)$$

$$= \sum_{(\chi''_i)_{i=1,\ldots,s} = \chi_0}^{(\chi''_i)_{i=1,\ldots,s} = \chi_0} \chi''_1 \chi_1(A_1) \cdots \chi''_s \chi_s(A_s) \sum_{u_1=1}^{p^m} \cdots \sum_{u_s=1}^{p^m} \chi'_1(u_1) \cdots \chi'_s(u_s), \quad (3.21)$$

and (3.18) is clear. Note, if $\chi_i$ is primitive mod $p^m$ then $\chi'_i \chi''_i$ must be primitive for all $\chi''_i$ mod $p^m$ with $(\chi''_i)_{i=1,\ldots,s} = \chi_0$ (since $\chi_i = (\chi'_i \chi''_i)^{k_i}$).

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

$$J_1 = p^{-(m-n)} \sum_{(\chi''_i)_{i=1,\ldots,s} = \chi_0}^{(\chi''_i)_{i=1,\ldots,s} = \chi_0} G \left( \prod_{j=1}^{s} \chi'_j \chi''_j p^{m-n} \right) \prod_{i=1}^{s} \chi'_i \chi''_i (A_i^{-1} B') G (\chi'_i \chi''_i, p^m), \quad (3.22)$$

where the * indicates the sum is restricted to the $\chi''_i$ 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 $(\chi''_i)_{i=1,\ldots,s} = \chi_0$, that is $c_{\phi(p^m)}(c''_i k_i) = 1$, and $p^{t_i} \mid k_i$, then

$$p^{m-t_i-1} \mid c''_i \Rightarrow p^{n+1} \mid c''_i. \quad (3.23)$$

Likewise for $p = 2$, if $(\chi''_i)_{i=1,\ldots,s} = \chi_0$ and $m \geq n + t + 3$, we have

$$2^{m-t-2} \mid c''_i \Rightarrow 2^{n+1} \mid c''_i. \quad (3.24)$$

Hence $p \mid (c'_i + c''_i)$ iff $p \mid c'_i$ and $p^n \mid \sum_{i=1}^{s} (c'_i + c''_i)$ iff $p^n \mid \sum_{i=1}^{s} c'_i$. That is $\chi'_i \chi''_i$ is primitive mod $p^m$ iff $\chi'_i$ 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 $\chi$ is not primitive mod $p^k$ we see that all the terms in (3.22) will be zero unless the $\chi_i'$ 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 $\chi$ is primitive mod $p^k$ gives the form (3.19).

\[ \square \]

### 3.2 Proof of Theorem 3.0.2

Suppose that $m \geq n + t + 2$ and at least one of the $\chi_i$ 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 $\chi_i'$ 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

\[ J_1 = p^{\frac{1}{2}(m(s-1)+n)} \sum_{(\chi_i'')^{k_i} = \chi_0} \frac{\chi_i'\chi_i''(A_1^{-1}B'(c_i' + c_i'')) \cdots \chi_s'\chi_s''(A_s^{-1}B'(c_s' + c_s''))}{\chi_1'\chi_1'' \cdots \chi_s'\chi_s''(v)} \tilde{\delta}, \tag{3.25} \]

where the

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

and

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

with $\epsilon_{p^m}$, and $r$ as defined in (3.13) and (3.12), with an extra factor $c_3(rv)$ 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

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

36
and so may be pulled out of the sum straight away. Suppose now that

\[ m \geq n + 2t + 2. \]  

(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 \( \chi''_i \) 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

\[
\chi''_i(c' + c''_i) = \chi''_i(c'_i), \quad \chi''_1 \cdots \chi''_s(v) = \chi''_1 \cdots \chi''_s(v').
\]  

(3.27)

We define the integers \( R_j \) by

\[
a^\phi(p^i) = 1 + R_j p^i. \]  

(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

\[
l_i = (c'_i)^{-1}(c''_i p^{-(m-t-1)})R_{m-t-1}^{-1} \mod p^m,
\]

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

\[
c'_i + c''_i \equiv c'_i (1 + l_i R_{m-t-1} p^{m-t-1}) \mod p^m
\equiv c'_i (1 + R_{m-t-1} p^{m-t-1})^{l_i} \mod p^m
\equiv c'_i a^{l_i \phi(p^{m-t-1})} \mod p^m,
\]

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

Similarly, noting that \( 2(m - n - t - 1) \geq m - n \),
\[
v = v' + p^{-n}(c_1'' + \cdots + c_s'') \\
\equiv v' \left( 1 + (v')^{-1} LR_{m-n-t-1} p^{m-n-t-1} \right) \mod p^m \\
\equiv v' a(v')^{-1} \phi(p^{m-t-n-1}) L \mod p^{m-n},
\]
and
\[
\chi_1' \chi_1'' \cdots \chi_s' \chi_s''(v) = \chi_1' \chi_1'' \cdots \chi_s' \chi_s''(v') e_{\phi(p^m)}(p^n v'(v')^{-1} \phi(p^{m-t-n-1}) L) \\
= \chi_1' \chi_1'' \cdots \chi_s' \chi_s''(v') e_{p^{t+1}}(L).
\] (3.30)

By substituting (3.29) and (3.30) in (3.25) we get
\[
J_1 = p^{\frac{1}{2}(m(s-1)+n)} \delta(\chi_1', \ldots, \chi_s') \sum_{(\chi_i')^{s_i} = \chi_0}^{(\chi_i'')^{s_i} = \chi_0} \frac{\chi_1' \chi_1''(A_1^{-1} B' c_1') \cdots \chi_s' \chi_s''(A_s^{-1} B' c_s')}{\chi_1' \chi_1'' \cdots \chi_s' \chi_s''(v')} \\
= p^{\frac{1}{2}(m(s-1)+n)} \delta(\chi_1', \ldots, \chi_s') \prod_{j=1}^{s} \chi_j'(A_j^{-1} B' c_j' v'^{-1}) \prod_{i=1}^{s} \sum_{(\chi_i'')^{s_i} = \chi_0} \chi_i''(A_i^{-1} B' c_i' v'^{-1}).
\] (3.31)

Clearly this sum is zero unless each \( A_i^{-1} B' c_i' v'^{-1} \) is a \( k_i \)-th power, when
\[
J_1 = D_1 \cdots D_s p^{\frac{1}{2}(m(s-1)+n)} \delta(\chi_1', \ldots, \chi_s') \prod_{i=1}^{s} \chi_i'(A_i^{-1} B' c_i' v'^{-1}). \quad \square
\]
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 $\delta$ now defined by

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

where $c_i, v, \omega$ are defined as

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

and

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

**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 $\chi'_i$ 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 $\alpha_i$, then

$$J_1 = 2^4(m(s-1)+n)D_1 \cdots D_s \chi_1(\alpha_1) \cdots \chi_s(\alpha_s) \delta(\chi'_1, \ldots, \chi'_s), \quad (3.35)$$

where the $c'_i$ are defined by $\chi'_i(5) = e^{2m-2c'_i}$, $v' = 2^{-n} \sum_{i=1}^{s} c'_i$ and $\delta(\chi'_1, \ldots, \chi'_s)$ is as in (3.32) with $c'_i$ and $v'$ replacing the $c_i$ and $v$.

Otherwise $J_1 = 0$.

**Proof.** Suppose first that $m \geq n + t + 5$ and at least one of the $\chi_i$ 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 $\chi'_i$ 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

\[
\mathcal{J}_1 = 2^{\frac{1}{2}(m(s-1)+n)} \sum_{(\chi_i'\chi''_1)^k=\chi_0} \frac{\chi_1'\chi''_1(A_1^{-1}B'(c_i' + c_i'')) \cdots \chi_s'\chi''_s(A_s^{-1}B'(c_s' + c_s''))}{\chi_1'\chi''_1 \cdots \chi_s'\chi''_s(v)} \delta, \tag{3.36}
\]

where the

\[\chi_i'\chi''_1(5) = c_{2m-2}(c_i' + c_i''), \quad v = 2^{-n} \sum_{i=1}^s (c_i' + c_i''),\]

and

\[
\tilde{\delta} = \delta(\chi_1'\chi''_1, \ldots, \chi_s'\chi''_s) = \left(\frac{2}{v}\right)^{m-n} \left(\prod_{i=1}^s (c_i' + c_i'')\right)^m \omega^{(2^n-1)v}.
\]

From \((\chi_i'')^{k_i} = 1\) we have \(e_{2m-2}(c_i''k_i) = 1\) and \(2^{m-2}|c_i''\). Hence

\[c_i' + c_i'' \equiv c_i' \mod 2^{m-t-2}, \tag{3.37}\]

and

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

So for \(m \geq n + t + 5\) we have \(c_i' + c_i'' \equiv c_i' \mod 8, v \equiv v' \mod 8,\) 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 \(2^{m-t-2} | c_i''\) we know that the \(\chi_i''\) are all mod \(2^{t+2}\) characters. Suppose now that \(m \geq 2t + n + 4.\) Then (3.37) and (3.38) give \(c_i' + c_i'' \equiv c_i' \mod 2^{t+2}, v \equiv v' \mod 2^{t+2},\) and

\[\chi_i''(c_i' + c_i'') = \chi_i''(c_i'), \quad \chi_i' \cdots \chi_s''(v) = \chi_i' \cdots \chi_s''(v').\]

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

\[5^{2^{j-2}} = 1 + R_j 2^j.\]
From $R_{i+1} \equiv R_i + 2^{i-1}R_i^2$ we have the relationship $R_j \equiv R_i \mod 2^{i-1}$ for all $j \geq i \geq 2$. Define a positive integer $l_i := (c'_i)^{-1}c''_i2^{-(m-t-2)}R_{m-t-2}^{-1} \mod 2^m$. Since $2(m - t - 2) \geq m$ we have

$$c'_i + c''_i \equiv c'_i \left(1 + l_iR_{m-t-2}2^{m-t-2} \right) \mod 2^m$$

$$\equiv c'_i \left(1 + R_{m-t-2}2^{m-t-2} \right)^{l_i} \mod 2^m$$

$$\equiv c'_i5^{l_i2^{m-t-4}} \mod 2^m,$$

and $\chi'_i(c'_i + c''_i) = \chi'_i(c'_i)e_{2t+2}(c'_i l_i)$. If $m \geq 2t + n + 5$, then

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

giving

$$\prod_{i=1}^{s} \chi'_i\chi''_i(c'_i + c''_i) = e_{2t+2}(L) \prod_{i=1}^{s} \chi'_i\chi''_i(c'_i), \quad L := R_{m-t-n-2}^{-1} \sum_{i=1}^{s} c''_i2^{-(m-t-2)}.$$

(3.39)

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

$$v = v' + 2^{-n}(c''_1 + \cdots + c''_s)$$

$$\equiv v' \left(1 + (v')^{-1}LR_{m-n-t-2}2^{m-n-t-2} \right)$$

$$\equiv v'5^{(v')^{-1}2^{m-n-t-4}L} \mod 2^m,$$

and

$$\chi'_1\chi''_1 \cdots \chi'_s\chi''_s(v) = \chi'_1\chi''_1 \cdots \chi'_s\chi''_s(v')e_{2t+2}(L).$$

(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 $p 
mid k_i$ for at least one $i$ and none of the $\chi_i$ 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

$$J_B(\vec{\chi}, h_1, p^m) = \sum_{u_1, \ldots, u_s = 1}^{p^{m-1}} \sum_{v_1, \ldots, v_s = 1}^{p} \chi_1(u_1) \cdots \chi_s(u_s),$$

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

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

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

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

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

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

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

and

$$J_B(\vec{\chi}, h_1, p^m) = p^{s-1} \sum_{u_1, \ldots, u_s = 1}^{p^{m-1}} \chi_1(u_1) \cdots \chi_s(u_s) = p^{s-1} J_B(\vec{\chi}, h_1, p^{m-1}).$$

If the $\chi_i$ 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:

$$J_B(\vec{\chi}, h_1, p^m) = p^s \sum_{x_1 = 1}^{p^{m-1}} \cdots \sum_{x_s = 1}^{p^{m-1}} \chi_1(x_1) \cdots \chi_s(x_s).$$

43
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

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

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

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

(4.2)
was evaluated in [18] \((p \text{ odd})\) and \([19] \,(p = 2)\) for \(m\) sufficiently large \((\text{for } m \geq 2 \text{ if } p \nmid 2ABk)\).

In \([15]\) an evaluation was obtained for the Jacobi type sums

\[
h(x_1, \ldots, x_s) = x_1 + \cdots + x_s + B,
\]

and in Chapter 3 for their generalization

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

for \(m\) sufficiently large \((\text{for } m \geq 2 \text{ when } p \nmid 2Bk_1 \cdots k_s)\).

Zhang and Wang recently showed in \([22]\) that \((4.1)\) has an explicit evaluation when

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

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

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

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

\[
h(x_1, \ldots, x_s) = A_1 x_1 + \cdots + A_s x_s + B x_1^{w_1} \cdots x_s^{w_s}, \quad p \nmid A_1 \cdots A_s,
\]

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

\[
k := 1 - w_1 - \cdots - w_s. \quad (4.6)
\]
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),

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

Hence it is enough here to consider

\[
h_2 = h_2(x_1, \ldots, x_s) := x_1 + \cdots + x_s + B x_1^{w_1} \cdots x_s^{w_s} \tag{4.7}
\]

and evaluate the sum

\[
J_2 := J(\vec{\chi}, h_2, p^m) = \sum_{x_1=1}^{p^m} \cdots \sum_{x_s=1}^{p^m} \chi_1(x_1) \cdots \chi_s(x_s) \chi(x_1 + \cdots + x_s + B x_1^{w_1} \cdots x_s^{w_s}). \tag{4.8}
\]

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

\[
B = p^n B_1, \quad p \nmid B_1, \quad p^t \mid | k. \tag{4.9}
\]

To obtain our evaluation we shall first show in \( \S 2 \) that the sum is zero unless

\[
\chi_1 \cdots \chi_s = \chi_*, \tag{4.10}
\]

for some mod \( p^{m-n} \) character \( \chi_* \). In \( \S 3 \) we write our sums in terms of Gauss sums, and then in \( \S 4 \) 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

\[
e_q(x) := e^{2\pi ix/q}, \tag{4.11}
\]

46
we define integers \( r := (a^{p-1} - 1)/p \), \( 1 \leq c, c_i \leq \phi(p^m) \), and \( 1 \leq c^* \leq \phi(p^{m-n}) \), by

\[
\chi(a) = e_{\phi(p^m)}(c), \quad \chi_i(a) = e_{\phi(p^m)}(c_i), \quad \chi^*_i(a) = e_{\phi(p^{m-n})}(c^*).
\] (4.12)

When \( p = 2 \), we similarly define the integers \( 1 \leq c, c_i \leq 2^{m-2} \), \( 1 \leq c^* \leq 2^{m-n-2} \) by

\[
\chi(5) = e_{2^{m-2}}(c), \quad \chi_i(5) = e_{2^{m-2}}(c_i), \quad \chi^*_i(5) = e_{2^{m-n-2}}(c^*).
\] (4.13)

Define also \( \lambda \) and \( \varepsilon_{p^m} \) as

\[
\lambda := -B_1 \prod_{i=1}^{s} (c_i c_i^{-1} + p^n w_i) \mod p^m, \quad \varepsilon_{p^m} := \begin{cases} 1, & \text{if } p^m \equiv 1 \mod 4, \\ i, & \text{if } p^m \equiv 3 \mod 4. \end{cases}
\] (4.14)

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

\[
m \geq 2t + n + 3\beta - 1, \quad \beta := \begin{cases} 1, & \text{if } p \text{ is odd}, \\ 2, & \text{if } p = 2. \end{cases}
\] (4.15)

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

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

where

\[
\delta := \left( \frac{2r}{p} \right)^{sm-n} \left( \frac{-1}{p} \right)^{sm} \left( \frac{c_i^{m-n} c^m \prod_{i=1}^{s} (c_i + w_i p^n c^*)^m}{p} \right)^{\varepsilon_{p^m}^{s-1} \varepsilon_{p^{m-n}}} \] (4.16)
for \( p \) odd, unless \( p^{m-n} = 3^3 \), \( n > 0 \) when an extra factor \( e_3(rc_\ast) \) is needed,

\[
\delta := \left( \frac{2}{c_r^{m-n} e_{\text{m}} \prod_{i=1}^{s}(c_i + w_i 2^n c_\ast) \text{m}} \right) e_8((2^n - 1)c_\ast) \tag{4.17}
\]

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 \( c_i, c, c_\ast \) and \( \varepsilon_{p^m} \) as defined in (4.12), (4.13) and (4.14).

Otherwise \( J_2 = 0 \).

### 4.1 Preliminaries

We first observe that it is natural to assume that \( \chi \) is a primitive character mod \( p^m \). If all the \( \chi_i \) and \( \chi \) are imprimitive mod \( p^m \), then for any polynomial \( h \) we can simply reduce (4.1) to a mod \( p^m-1 \) sum, \( J(\vec{\chi}, h, p^m) = p^s J(\vec{\chi}, h, p^{m-1}) \). If some \( \chi_i \) is primitive, then there is a \( u \equiv 1 \mod p^{m-1} \) with \( \chi_i(u) \neq 1 \), and if \( \chi \) is imprimitive mod \( p^m \), then the change of variable \( x_i \mapsto x_i u \) 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 \( \chi_0 \) is the principal character mod \( p^m \), and \( \vec{\chi}_\xi := (\chi, \chi_1, \ldots, \chi_{s-1}) \) and
Let $h_\xi := x_1 + \cdots + x_{s-1} + 1 + B$ have one less variable.

The following lemma shows that $J_2 = 0$ unless $\chi_1 \cdots \chi_s$ 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 $\chi_1 \cdots \chi_s = \chi_k$ for some mod $p^{m-n}$ character $\chi_s$ if (4.19) holds or $\chi_1 \cdots \chi_s = \chi_0$ if (4.19) does not hold.

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

$$J(\vec{\chi}, h_2, p^m) = \sum_{x_1=1}^{p^m} \cdots \sum_{x_s=1}^{p^m} \chi(x_1) \cdots \chi(x_s)(x_1 + \cdots + x_s + Bx_1^{w_1} \cdots x_s^{w_s} z^{-k})$$

$$= \tilde{\chi}(z) J(\vec{\chi}, h_2, p^m),$$

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

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

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

and $p^n(k,\phi(p^{m-n})) | \vec{c}$. Hence there is an integer $c_s$ satisfying $p^n k c_s \equiv \vec{c} \mod \phi(p^m)$, and

$$\tilde{\chi} = \chi_s^k$$

where $\chi_s$ is the mod $p^{m-n}$ character with $\chi_s(a) = e^{\phi(p^{m-n})(c_s)}$.

For $p = 2$ and $m \geq n + 2$, taking $z = 2^{m-n-2}/(k, 2^{m-n-2})$ and writing $\tilde{\chi}(5) = e_{2^{m-2}}(\vec{c})$, we similarly obtain that $2^n(k, 2^{m-n-2}) | \vec{c}$ and $2^n k c_s \equiv \vec{c} \mod 2^{m-2}$ has a solution $c_s$. Setting

$$\chi_s(5) = e_{2^{m-n-2}}(c_s), \quad \chi_s(-1) = \tilde{\chi}(-1),$$

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

49
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

\[
J := \sum_{x_1=1}^{q-1} \cdots \sum_{x_s=1}^{q-1} \chi_1(g_1) \cdots \chi_l(g_l) \chi(h_1 + B h_2)
\]

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

### 4.2 Writing \( J_2 \) in Terms of Gauss Sums

For a character \( \chi \mod p^m \) 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 \( k \)th 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 \( \chi \) 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 \( \chi_* \). Then

\[
J_2 = p^n \sum_{\chi'' \in \mathcal{Y}} \chi'' \chi_*(B_1) \frac{G(\chi'', \chi_*, p^{m-n}) \prod_{i=1}^s G(\chi_i(\chi'' \chi_*^{w_i})^{w_i}, p^m)}{G(\chi, p^m)}, \tag{4.22}
\]
where $\mathcal{Y}$ denotes the mod $p^{m-n}$ characters $\chi''$ with $(\chi'')^k = \chi_0$.

In particular, if

$$m > n + t + \beta,$$

(4.23)

then $J_2 = 0$ unless $\chi_*$ is a primitive mod $p^{m-n}$ character and the $\chi_i \chi_*^{w_i}$ are all primitive mod $p^m$ characters.

Proof. If $\chi$ is a primitive character mod $p^m$, then

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

(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 $\chi$ 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 $\chi_1 \cdots \chi_s = \chi_*^k$, gives

$$G(\chi, p^m) J_2 = \sum_{x=1}^{p^m} \overline{\chi}(x) \sum_{x_1=1}^{p^m} \cdots \sum_{x_s=1}^{p^m} \chi_1(x_1) \cdots \chi_s(x_s)e_{p^m}\left(x \left(\sum_{i=1}^{s} x_i + B \prod_{i=1}^{s} x_i^{w_i}\right)\right)$$

$$= \sum_{x=1}^{p^m} \sum_{x_1=1}^{p^m} \cdots \sum_{x_s=1}^{p^m} \overline{\chi_1} \cdots \overline{\chi_s}(x) \chi_1(x_1) \cdots \chi_s(x_s)e_{p^m}\left(\sum_{i=1}^{s} x_i + B x_k \prod_{i=1}^{s} x_i^{w_i}\right)$$

$$= \sum_{x=1}^{p^m} \sum_{x_1=1}^{p^m} \cdots \sum_{x_s=1}^{p^m} \overline{\chi_1}(x) \cdots \overline{\chi_s}(x)e_{p^m}\left( B x_k \prod_{i=1}^{s} x_i^{w_i}\right) \prod_{i=1}^{s} \chi_i(x_i)e_{p^m}(x_i).$$

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

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

(4.25)

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

$$G(\chi, p^m) J_2 = \sum_{(\chi')^k = \chi_0 \mod p^m} \sum_{u=1}^{p^m} \sum_{x_1=1}^{p^m} \cdots \sum_{x_s=1}^{p^m} \chi'' \chi_s(u) e_{p^m} \left( p^n B_1 u \prod_{i=1}^{s} x_i^{w_i} \right) \prod_{i=1}^{s} \chi_i(x_i)e_{p^m}(x_i),$$

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

$$G(\chi, p^m) J_2 = \sum_{(\chi')^k = \chi_0 \mod p^m} \chi'' \chi_s(B_1) \sum_{u=1}^{p^m} \chi'' \chi_s(u) e_{p^m} \left( p^n u \right) \prod_{i=1}^{s} G(\chi_i(\chi'')^{w_i}, p^m).$$

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

$$\sum_{u=1}^{p^m} \chi'' \chi_s(u) e_{p^m} \left( p^n u \right) = p^j \sum_{u=1}^{p^{m-j}} \chi'' \chi_s(u) e_{p^{m-j}} \left( p^n u \right) = 0. \quad (4.26)$$

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

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

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

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

Hence for all the $\chi''$, we have that $\chi'' \chi_s$ is primitive mod $p^{m-n}$ iff $\chi_*$ is primitive mod $p^{m-n}$ and $\chi_i(\chi'' \chi_s)^{w_i}$ is primitive mod $p^m$ iff $\chi_i \chi_s^{w_i}$ is primitive mod $p^m$. Observing that $G(\chi, p^j) = 0$ if $\chi$ is an imprimitive character mod $p^j$ and $j \geq 2$, we deduce that $J_2 = 0$ unless $\chi_*$ is primitive mod $p^{m-n}$ and the $\chi_i \chi_s^{w_i}$ are primitive mod $p^m$. 

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

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

$$5^{2j-2} = 1 + R_j 2^j,$$  \hfill (4.29)

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

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

$$G(\chi, p^m) = p^{m/2} \chi(-c R_j^{-1}) \varepsilon_p m \left( \frac{2r}{p} \right)^m \varepsilon_{p^m}, \quad \text{if } p \neq 2, p^m \neq 27$$

$$= \left( \frac{2}{c} \right)^m \omega^c, \quad \text{if } p = 2 \text{ and } m \geq 5,$$  \hfill (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 $\varepsilon_{p^m}$ 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 $\chi \chi_1 \cdots \chi_s = \chi_s^k$ for some primitive mod $p^{m-n}$ character $\chi_s$ with the $\chi_i \chi_s^{w_i}$ all primitive mod $p^m$ (else the sum is zero). With $\beta$ and $c''$ as in (4.15) and (4.27), we have $p^{m-n-t-\beta} \mid c''$ and $\chi''$ is a mod $p^{t+\beta}$ character. In particular, since $m - n - t - \beta \geq t + \beta$, we have

$$\overline{\chi''}(c'' + c_s) = \overline{\chi''}(c_s).$$  \hfill (4.31)
Let $l_1$ be a positive integer with

$$l_1 \equiv c^{-1} c'' R_{m-1}^\frac{1}{p} \left( m - n - t - \beta \right) \mod p^{t+\beta}.$$

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

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

$$\equiv c_* \left( 1 + R_{m-n-t-\beta} p^{m-n-t-\beta} \right)^{l_1} \mod p^{m-n}$$

$$\equiv c_* \begin{cases} a^{l_1 \phi(p^{m-n-t-1})} \mod p^{m-n}, & \text{for } p \text{ odd}, \\ 5^{l_1 2^{m-n-t-4}} \mod 2^{m-n}, & \text{for } p = 2. \end{cases}$$

Hence,

$$\overline{\chi^*}(c'' + c_*) = \overline{\chi^*}(c_*) e_{pt+\beta} (-c_* l_1) = \overline{\chi^*}(c_*) e_{p^{m-n}} (-c'' R_{m^{-1}}),$$

and by (4.30) we have

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

(4.32)

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

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

(4.33)
Similarly, since $2(m - t - \beta) \geq m$, we have

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

where $l_2$ is a positive integer with

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

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

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

Hence, using Lemma (4.2.1), we get

$$G(\chi_i (\chi' \chi^*)^{w_i}, p^m) = p^m \chi_i (\chi' \chi^*)^{w_i} (-\beta + w_i p^n c*) e_{p^m} (-\beta + w_i p^n c*) e_{p^m} (\delta_c).$$

(4.34)

where

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

(4.35)

For $c$ defined as in (4.12) we have

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

(4.36)
where

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

(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

\[ \chi'' \chi_s (-c_0 R_{m-1}^{-1}) \chi'(\chi'' \chi_s)^{w_i} (-c_0 R_{m-1}^{-1}) = 1. \]

Since \( c \) is defined mod \( \phi(p^m) \) we can replace \( c \) by \( c = kp^n c_0 - \sum_{i=1}^s c_i \), and then

\[ e_{p^m}(p^n c_0 R_{m-1}^{-1}) e_{p^m}(-c R_{m-1}^{-1}) \prod_{i=1}^s e_{p^m}(-c_i + w_i p^n c_0) R_{m-1}^{-1} = 1, \]

with \(-c_0 + \sum_{i=1}^s (c_i + w_i 2^n c_0) + c = (2^n - 1)c_0 \) when \( p = 2 \). By substituting (4.32), (4.34), and (4.36) in (4.22) we get, for \( p^m \) and \( p^{m-n} \neq 3^3 \),

\[ J_2 = p^{\frac{m+n}{2}} \sum_{(\chi'')^k = \chi_0 \mod p^{m-n}} \delta \chi'' \chi_s (-B_1) \chi(-cc_0^{-1}) \prod_{i=1}^s \chi_i(\chi'' \chi_s)^{w_i} (c_i c_0^{-1} + w_i p^n) \]

\[ = p^{\frac{m+n}{2}} \delta \chi_s(\lambda) \chi(-cc_0^{-1}) \prod_{i=1}^s \chi_i(c_i c_0^{-1} + w_i p^n) \sum_{(\chi''')^k = \chi_0 \mod p^{m-n}} \chi''(\lambda), \]

with \( \lambda \) 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 \( \delta \) given in (4.16) for \( p \) odd and (4.17) for \( p = 2 \). If \( \lambda \) is a \( k \)th power mod \( p^{m-n} \), then (4.25) and \( (k, \phi(p^{m-n})) = (k, p - 1)p^t \) give

\[ J_2 = (k, p - 1)p^{\frac{m+n}{2} + \alpha} \delta \chi_s(\lambda) \chi(-cc_0^{-1}) \prod_{i=1}^s \chi_i(c_i c_0^{-1} + w_i p^n), \]

56
with $\alpha$ as in (4.18). If $\lambda$ is not a $k$th power mod $p^{m-n}$, then

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

and $J_2 = 0$. For $p^{m-n} = 3^3, n > 0$ we pick up an extra factor $e_3(rc_*)$ from $G(\chi''\chi_*, p^{m-n})$. When $p^m = 3^3$ the additional factors in the Gauss sums cancel.
Bibliography


