EVALUATING PRIME POWER GAUSS AND JACOBI SUMS

MISTY LONG, VINCENT PIGNO, AND CHRISTOPHER PINNER

Abstract. We show that for any mod $p^m$ characters, $\chi_1, \ldots, \chi_k$, the Jacobi sum,
\[
\sum_{x_1 = 1}^{p^m} \cdots \sum_{x_k = 1}^{p^m} \chi_1(x_1) \cdots \chi_k(x_k),
\]
has a simple evaluation when $m$ is sufficiently large (for $m \geq 2$ if $p \nmid B$). As part of the proof we give a simple evaluation of the mod $p^m$ Gauss sums when $m \geq 2$.

1. Introduction

For multiplicative characters $\chi_1$ and $\chi_2$ mod $q$ one defines the classical Jacobi sum by
\[
J(\chi_1, \chi_2, q) := \sum_{x=1}^{q} \chi_1(x) \chi_2(1-x).
\]
More generally for $k$ characters $\chi_1, \ldots, \chi_k$ mod $q$ one can define
\[
J(\chi_1, \ldots, \chi_k, q) = \sum_{x_1 = 1}^{q} \cdots \sum_{x_k = 1}^{q} \chi_1(x_1) \cdots \chi_k(x_k).
\]

If the $\chi_i$ are mod $rs$ characters with $(r, s) = 1$ then, writing $\chi_i = \chi_i' \chi_i''$ where $\chi_i'$ and $\chi_i''$ are mod $r$ and mod $s$ characters respectively, it is readily seen (e.g. [12, Lemma 2]) that
\[
J(\chi_1, \ldots, \chi_k, rs) = J(\chi_1', \ldots, \chi_k', r)J(\chi_1'', \ldots, \chi_k'', s).
\]

Hence, one usually only considers the case of prime power moduli $q = p^m$.

Zhang & Yao [11] showed that the sums (1) can in fact be evaluated explicitly when $m$ is even (and $\chi_1, \chi_2$ and $\chi_1 \chi_2$ are primitive mod $p^m$). Working with a slightly more general binomial character sum the authors [9] showed that techniques of Cochrane & Zheng [3] can be used to obtain an evaluation of (1) for any $m > 1$ ($p$ an odd prime). Zhang and Xu [12] considered the general case, (2), obtaining (assuming that $\chi, \chi^{n_1}, \ldots, \chi^{n_k}$, and $\chi^{n_1 + \cdots + n_k}$ are primitive characters modulo $p^m$)
\[
J(\chi^{n_1}, \ldots, \chi^{n_k}, p^m) = p^{\frac{k}{2}(k-1)m} \sum (u^n) \chi(u^{n_1} \ldots n_k), \quad u := n_1 + \cdots + n_k,
\]

\begin{flushleft}
\textit{Date:} November 20, 2013.
\textit{1991 Mathematics Subject Classification.} Primary: 11L05; Secondary: 11L03, 11L10.
\textit{Key words and phrases.} Exponential sums, Gauss sums.
\end{flushleft}
when $m$ is even, and when the $m,k,n_1,\ldots,n_k$ are all odd

$$J(\chi^{n_1},\ldots,\chi^{n_k},p^m) = p^{\frac{k(k-1)}{2}m} \chi(u^n) \chi(n_1^{n_1} \cdots n_k^{n_k}) \left( \frac{\epsilon_{m,n_k}}{p} \right),$$

if $p \neq 2$;

$$J(\chi^{n_1},\ldots,\chi^{n_k},p^m) = \frac{2^{k-1}}{m_{n_1 \cdots n_k}^n},$$

if $p = 2$,

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

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

In this paper we give an evaluation for all $m > 1$ (i.e. irrespective of the parity of $k$ and the $n_i$). In fact we evaluate the slightly more general sum

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

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

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

For example $J_B(\chi_1,\ldots,\chi_k,p^m) = \chi_1 \cdots \chi_k(B) J(\chi_1,\ldots,\chi_k,p^m)$ when $p \nmid B$. From the change of variables $x_i \mapsto -x_k x_i, 1 \leq i < k$ one also sees that

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

where $\chi_0$ denotes the principal character, so we assume that $B = p^n$ with $n < m$.

**Theorem 1.1.** Let $p$ be a prime and $m \geq n + 2$. Suppose that $\chi_1,\ldots,\chi_k$ are $k \geq 2$ characters mod $p^m$ with at least one of them primitive.

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

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

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

where for $p$ odd

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

and for $p = 2$ and $m-n \geq 5$,

$$\delta = \left( \frac{2}{v} \right)^{m-n} \left( \frac{2}{c_1 \cdots c_k} \right)^m \omega^{(2^{n-1})v},$$

with $\epsilon_{p^m}$ as defined in (5), the $r$ and $c_i$ as in (11) and (13) or (14) below, and

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

For $m \geq 5$ and $m-n = 2,3$ or 4 the formula (7) for $\delta$ should be multiplied by $\omega$, $\omega^{2^m-1}$ or $\omega^{2^m-1} \chi_k(-1) \omega^{2v}$ respectively.
Of course it is natural to assume that at least one of the $\chi_1, \ldots, \chi_k$ is primitive, otherwise we can reduce the sum to a mod $p^{m-1}$ sum. For $n = 0$ and $\chi_1, \ldots, \chi_k$ and $\chi_1 \cdots \chi_k$ all primitive mod $p^m$ our result simplifies to

$$J(\chi_1, \ldots, \chi_k, p^m) = \frac{\prod_{i,j=1}^k \chi_i(c_i)\chi_j(c_j)}{\chi_1 \cdots \chi_k(v)} \delta, \quad v = c_1 + \cdots + c_k,$$

with

$$\delta = \begin{cases} 1, & \text{if } m \text{ is even,} \\ \left(\frac{-2\pi c}{\ell p}\right)^{k-1}, & \text{if } m \text{ is odd and } p \neq 2, \\ 2, & \text{if } m \geq 5 \text{ is odd and } p = 2. \end{cases}$$

In the remaining $n = 0$ case, $p = 2$, $m = 3$ we have $J(\chi_1, \ldots, \chi_k, 2^3) = 2^{\frac{1}{2}(k-1)(-1)^{\ell/2}}$ where $\ell$ denotes the number of characters $1 \leq i \leq k$ with $\chi_i(-1) = -1$.

When the $\chi_i = \chi^{n_i}$ for some primitive mod $p^m$ character $\chi$ we can write $c_i = n_i c$ (where $c$ is determined by $\chi(n)$ as in (13) or (14)) and we recover the form (3) and (4) with the addition of a factor $\left(\frac{-2\pi c}{\ell p}\right)^{k-1}$ for $p \neq 2$, $m$ odd, which of course can be ignored when $k$ is odd as assumed in [12].

For completeness we observe that in the few remaining cases $m \geq n + 2$ cases (6) becomes

$$J_{p^m}(\chi_1, \ldots, \chi_k, p^m) = 2^{\frac{1}{2}(m(k-1)+n)} \begin{cases} -i\omega^{k-\sum_{i=1}^k \chi_i(-1)}, & \text{if } m = 3, n = 1, \\ \omega^{k-\sum_{i=1}^k \chi_i(-1)-1} \prod_{i=1}^k \chi_i(c_i), & \text{if } m = 4, n = 1, \\ i^{1-v} \prod_{i=1}^k \chi_i(c_i), & \text{if } m = 4, n = 2. \end{cases}$$

Our proof of Theorem 1.1 involves expressing the Jacobi sum (2) in terms of classical Gauss sums

$$(9) \quad G(\chi, p^m) := \sum_{x=1}^{p^m} \chi(x)e_{p^m}(x),$$

where $\chi$ is a mod $p^m$ character and $e_{p^m}(x) := e^{2\pi ix/p}$. Writing (1) in terms of Gauss sums is well known for the mod $p$ sums and the corresponding result for (2) can be found, along with many other properties of Jacobi sums, in Berndt, R. J. Evans and K. S. Williams [1, Theorem 2.1.3 & Theorem 10.3.1 ] or Lidl-Niederreiter [5, Theorem 5.21]. There the results are stated for sums over finite fields, $\mathbb{F}_{p^m}$, so it is not surprising that such expressions exist in the less studied mod $p^m$ case. When $\chi_1, \ldots, \chi_k$ and $\chi_1 \cdots \chi_k$ are primitive, Zhang & Yao [11, Lemma 3] for $k = 2$, and Zhang and Xu [12, Lemma 1] for general $k$, showed that

$$(10) \quad J(\chi_1, \ldots, \chi_k, p^m) = \frac{\prod_{i=1}^k G(\chi_i, p^m)}{G(\chi_1 \cdots \chi_k, p^m)}.$$ 

In Theorem 2.2 we obtain a similar expansion for $J_{p^m}(\chi_1, \ldots, \chi_k, p^m)$. As we show in Theorem 2.1 the mod $p^m$ Gauss sums can be evaluated explicitly using the method of Cochrane and Zheng [3] when $m \geq 2$.

For $m = n + 1$ (with at least one $\chi_i$ primitive) the Jacobi sum is still zero unless all the $\chi_i$ are primitive mod $p^m$ and $\chi_1 \cdots \chi_k$ is a mod $p$ character. Then we can say that $|J_{p^m}(\chi_1, \ldots, \chi_k, p^m)| = p^{\frac{1}{2}(nk-1)}$ if $\chi_1 \cdots \chi_k$ is $\chi_0$ and $p^{\frac{1}{2}(mk-1)}$ otherwise, but an explicit evaluation in the latter case is equivalent to an explicit evaluation of the mod $p$ Gauss sum $G(\chi_1 \cdots \chi_k, p)$ when $m \geq 2$. 
2. Gauss Sums

In order to use the result from [4] we must first define some terms. For $p$ odd let $a$ be a primitive root mod $p^m$. We define the integers $r$, and $R_j$ by

\begin{equation}
\alpha^{\phi(p)} = 1 + rp, \quad \alpha^{\phi(p')} = 1 + R_j p^j.
\end{equation}

Note, $p \nmid r$ and for $j \geq i$,

\begin{equation}
R_j \equiv R_i \mod p^i.
\end{equation}

For a character $\chi$, mod $p^m$ we define $c_i$ by

\begin{equation}
\chi_i(a) = e_{\phi(p^m)}(c_i),
\end{equation}

with $1 \leq c_i \leq \phi(p^m)$. Note, $p \nmid c_i$ exactly when $\chi_i$ is primitive. For $p = 2$ and $m \geq 3$ we need two generators $-1$ and $a = 5$ for $\mathbb{Z}_2^{2m}$ and define $R_j$, $j \geq 2$, and $c_i$ by

\begin{equation}
a^{2i-2} = 1 + R_j 2^j, \quad \chi_i(a) = e_{2m-2}(c_i),
\end{equation}

with $\chi_i$ primitive exactly when $2 \nmid c_i$. Noting that $R_j^2 \equiv 1 \mod 8$, we get

\begin{equation}
R_{i+1} = R_i + 2^{i-1} R_j^2 \equiv R_i + 2^{i-1} \mod 2^{i+2}.
\end{equation}

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

\begin{equation}
R_j \equiv R_{i+2} \equiv R_{i+1} + 2^i \equiv (R_i + 2^{i-1}) + 2^i \equiv R_i - 2^{i-1} \mod 2^{i+1}
\end{equation}

and

\begin{equation}
R_j \equiv (R_{i-1} + 2^{i-2}) - 2^{i-1} \equiv R_{i-1} - 2^{i-2} \mod 2^{i+1}.
\end{equation}

We shall need an explicit evaluation of the mod $p^m$, $m \geq 2$, Gauss sums. The form we use comes from applying the technique of Cochrane & Zheng [3] as formulated in [8]. For odd $p$ this is essentially the same as [4, §9] but for $p = 2$ seems new. Variations can be found in Odoni [7] and Mauclaire [6] (see also [1, Chapter 1]).

**Theorem 2.1.** Suppose that $\chi$ is a mod $p^m$ character with $m \geq 2$. If $\chi$ is imprimitive, then $G(\chi, p^m) = 0$. If $\chi$ is primitive, then

\begin{equation}
G(\chi, p^m) = \frac{p^m}{2^m} \chi \left( -c R_j^{-1} \right) e_{p^m} \left( -c R_j^{-1} \right) \left( \frac{-2r}{p} \right)^m \epsilon_{p^m}, \quad \text{if } p \neq 2,
\end{equation}

\begin{equation}
\left( \frac{2}{p} \right)^m \omega^c, \quad \text{if } p = 2 \text{ and } m \geq 5,
\end{equation}

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

For the remaining cases

\begin{equation}
G(\chi, 2^m) = \frac{2^m}{2^m} \left\{ \begin{array}{ll}
i \omega^{1-\chi(-1)}, & \text{if } m = 2, \\
\chi(-c) e_{16}(-c), & \text{if } m = 4.
\end{array} \right.
\end{equation}

Here $x^{-1}$ denotes the inverse of $x$ mod $p^m$, and $r$, $R_j$ and $c$ are as in (11) and (13) or (14) and $\omega$ as in (8).

**Proof.** When $p$ is odd [8, Theorem 2.1] gives

\begin{equation}
G(\chi, p^m) = \frac{p^{m/2}}{2^m} \chi(\alpha) e_{p^m}(\alpha) \left( \frac{-2r}{p^m} \right) \epsilon_{p^m}
\end{equation}
where \(\alpha\) is a solution of
\[
2 + R_j \alpha \equiv 0 \pmod{p^J}, \quad J := \left\lfloor \frac{m}{2} \right\rfloor,
\]
(and zero if no solution exists). If \(p \nmid c\) there is no solution and \(G(\chi, p^m) = 0\). If \(p \nmid c\) by (12) we may take \(\alpha = -cR_j^{-1} \equiv -cR_j^{-1} \pmod{p^J}\) for any \(j \geq J\). If \(p = 2,\ m \geq 6,\) and \(\chi\) is primitive, then [8, Theorem 5.1] gives
\[
G(\chi, p^m) = 2^{m/2} \chi(\alpha) e_2(m) \left\{ \begin{array}{ll}
1, & \text{if } m \text{ is even},
\frac{1 + (-1)^{\lambda_i R_j c}}{\sqrt{2}}, & \text{if } m \text{ is odd},
\end{array} \right.
\]
where \(\alpha\) is a solution to
\[
c + R_j \alpha \equiv 0 \pmod{2^{J+1}},
\]
and \(c + R_j \alpha = 2^{\left\lfloor \frac{J+1}{2} \right\rfloor} \lambda\) (and zero if there is no solution or \(\chi\) is imprimitive). If \(2 | c\) and \(j \geq J + 2\) then (using (16) and \(R_j \equiv -1 \pmod{4}\)) we can take
\[
\alpha \equiv -cR_j^{-1} \equiv -c(R_j + 2^{J-1})^{-1} \equiv -c(R_j^{-1} - 2^{J-1}) \pmod{2^{J+1}},
\]
and
\[
\chi(\alpha) e_2(m) = \chi(-cR_j^{-1}) e_2(m) (-cR_j^{-1}) \chi(1 - R_j 2^{J-1}) e_2(m) (c 2^{J-1}),
\]
where, checking the four possible \(c \pmod{8}\),
\[
\left( \frac{1 + (-1)^{\lambda_i R_j c}}{\sqrt{2}} \right) = \left( \frac{1 - i^c}{\sqrt{2}} \right) = \omega^{-c} \left( \frac{2}{c} \right).
\]
Now
\[
e_2(m)(c 2^{J-1}) = e_2(m - z)(c 2^{J-3}) = \chi \left( 5^{2^{J-3}} \right) = \chi \left( 1 + R_{J-1} 2^{J-1} \right),
\]
where, since \(R_j \equiv R_{J-1} - 2^{J-2} \pmod{2^{J+1}},\)
\[
(1 - R_j 2^{J-1}) (1 + R_{J-1} 2^{J-1}) = 1 + (R_{J-1} - R_j) 2^{J-1} - R_j R_{J-1} 2^{2J-2} \\
\equiv 1 + 2^{2J-3} + R_{J-1} 2^{2J-2} \equiv 1 + R_{J-1} 2^{2J-3} \equiv 2^{2J-3} \equiv 2^{2J-5} \pmod{2}.
\]
Hence
\[
\chi(1 - R_j 2^{J-1}) e_2(m)(c 2^{J-1}) = \chi \left( 5^{2^{J-5}} \right) = e_2(m - z)(c 2^{J-5}) = \left\{ \begin{array}{ll}
\omega^c, & \text{if } m \text{ is even},
\omega^{2c}, & \text{if } m \text{ is odd}.
\end{array} \right.
\]
One can check numerically that the formula still holds for the \(2^{m-2}\) primitive mod \(2^m\) characters when \(m = 5\). For \(m = 2, 3, 4\) one has (19) instead of \(2i\omega, 2^2 i\omega^2, 2^2\chi(e)(e)\omega^c\) (so our formula (18) requires an extra factor \(\omega^{-1}, \omega^{-1}(\chi(-1))\) or \(\chi(-1)\omega^{-2c}\) respectively).

We shall need the counterpart of (10) for the \(J_{p^m}(\chi_1, \ldots, \chi_k)\). We state a less symmetrical version to allow weaker assumptions on the \(\chi_i\):

**Theorem 2.2.** Suppose that \(\chi_1, \ldots, \chi_k\) are characters \(\pmod{p^m}\) with \(m > n\) and \(\chi_k\) primitive \(\pmod{p^m}\). If \(\chi_1 \cdots \chi_k\) is a mod \(p^{m-n}\) character, then
\[
J_{p^m}(\chi_1, \ldots, \chi_k, \chi) = p^n \frac{G(\chi_1 \cdots \chi_k, \chi, p^{m-n})}{G(\chi_k, p^m)} \prod_{i=1}^{k-1} G(\chi_i, p^m).
\]
If \(\chi_1 \cdots \chi_k\) is not a mod \(p^{m-n}\) character, then \(J_{p^m}(\chi_1, \ldots, \chi_k, \chi) = 0\).
From well known properties of Gauss sums (see for example Section 1.6 of [1]),

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

when \( \chi_1 \cdots \chi_k \) is a primitive mod \( p^{m-n} \) character and at least one of the \( \chi_i \) is a primitive mod \( p^m \) character we immediately obtain the symmetric form

\begin{equation}
J_{p^m}(\chi_1, \ldots, \chi_k, p^m) = \frac{\prod_{i=1}^k G(\chi_i, p^m)}{G(\chi_1 \cdots \chi_k, p^{m-n})}.
\end{equation}

In particular we recover (10) under the sole assumption that \( \chi_1 \cdots \chi_k \) is a primitive mod \( p^m \) character.

\textbf{Proof.} We first note that if \( \chi \) is a primitive character mod \( p^j \), \( j \geq 1 \), then

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

Indeed, for \( p \nmid A \) this is plain from \( y \mapsto A^{-1}y \). If \( p \mid A \) and \( j = 1 \) the sum equals \( \sum_{y=1}^{p} \chi(y) = 0 \). For \( j \geq 2 \) as \( \chi \) is primitive there exists a \( z \equiv 1 \mod p^{j-1} \) with \( \chi(z) \neq 1 \), (there must be some \( a \equiv b \mod p^{j-1} \) with \( \chi(a) \neq \chi(b) \), and we can take \( z = ab^{-1} \)) so

\begin{equation}
\sum_{y=1}^{p^j} \chi(y)e_{p^j}(Ay) = \sum_{y=1}^{p^j} \chi(zy)e_{p^j}(Azy) = \chi(z) \sum_{y=1}^{p^j} \chi(y)e_{p^j}(Ay)
\end{equation}

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

Hence if \( \chi_k \) is a primitive character mod \( p^m \) we have

\begin{align*}
\chi_k(-1)G(\chi_k, p^m) \sum_{x_1=1}^{p^m} \cdots \sum_{x_{k-1}=1}^{p^m} \chi_1(x_1) \cdots \chi_{k-1}(x_{k-1}) \chi_k(p^m - x_1 - \cdots - x_{k-1}) \\
= \chi_k(-1) \sum_{x_1=1}^{p^m} \cdots \sum_{x_{k-1}=1}^{p^m} \chi_1(x_1) \cdots \chi_{k-1}(x_{k-1}) \sum_{y=1}^{p^m} \chi_k(y)e_{p^m}((p^m - x_1 - \cdots - x_{k-1})y) \\
= \sum_{y=1}^{p^m} \chi_k(-y)e_{p^m}(p^m y) \left( \sum_{x_1=1}^{p^m} \chi_1(x_1)e_{p^m}(-x_1 y) \cdots \sum_{x_{k-1}=1}^{p^m} \chi_{k-1}(x_{k-1})e_{p^m}(-x_{k-1} y) \right) \\
= \sum_{y=1}^{p^m} \chi_1 \cdots \chi_k(-y)e_{p^m}(p^m y) \left( \sum_{x_1=1}^{p^m} \chi_1(x_1)e_{p^m}(x_1) \cdots \sum_{x_{k-1}=1}^{p^m} \chi_{k-1}(x_{k-1})e_{p^m}(x_{k-1}) \right) \\
= \chi_1 \cdots \chi_k(-1) \sum_{y=1}^{p^m} \chi_1 \cdots \chi_k(y)e_{p^m}(p^m y) \prod_{i=1}^{k-1} G(\chi_i, p^m).
\end{align*}
If \( m > n \) and \( \chi_1 \cdots \chi_k \) is a mod \( p^{m-n} \) character, then
\[
\sum_{y=1 \atop p \nmid y}^{p^m} \chi_1 \cdots \chi_k (y) e_{p^m} (p^n y) = p^n \sum_{y=1 \atop p \nmid y}^{p^{m-n}} \chi_1 \cdots \chi_k (y) e_{p^{m-n}} (y) = p^n G(\chi_1 \cdots \chi_k, p^{m-n}).
\]

If \( \chi_1 \cdots \chi_k \) is a primitive character mod \( p^j \) with \( m - n < j \leq m \), then by the same reasoning as in (25)
\[
\sum_{y=1 \atop p \nmid y}^{p^m} \chi_1 \cdots \chi_k (y) e_{p^m} (p^n y) = p^{m-j} \sum_{y=1}^{p^j} \chi_1 \cdots \chi_k (y) e_{p^j} (p^{j-(m-n)} y) = 0
\]
and the result follows on observing that
\[
\overline{G(\chi, p^m)} = \chi(-1) G(\chi, p^m).
\]

\[\Box\]

3. Proof of Theorem 1.1

We assume that \( \chi_1, \ldots, \chi_k \) are all primitive mod \( p^m \) characters and \( \chi_1 \cdots \chi_k \) is a primitive mod \( p^{m-n} \) character, since otherwise from Theorem 2.2 and (23), \( J_{p^n} (\chi_1, \ldots, \chi_k, p^m) = 0 \). In particular we have (24).

Writing \( R = R_{\lceil \frac{m}{2} \rceil + 2} \) then by (24) and the evaluation of Gauss sums in Theorem 2.1 we have
\[
J_{p^n} (\chi_1, \ldots, \chi_k, p^m) = \prod_{i=1}^{k} G(\chi_i, p^m) / G(\chi_1 \cdots \chi_k, p^{m-n})
\]
\[
= \prod_{i=1}^{k} p^{m/2} \chi_i (-c_i R^{-1}) e_{p^m} (-c_i R^{-1}) \delta_i
\]
\[
= p^{\frac{1}{2} (a (k-1) + n)} \prod_{i=1}^{k} \chi_i (c_i) \delta_s^{-1} \prod_{i=1}^{k} \delta_i,
\]
(26)

where
\[
\delta_i = \begin{cases} 
\left( \frac{-2c_i}{p} \right)^m e_{p^m}, & \text{if } p \text{ is odd, } p \neq 2, \\
\left( \frac{2}{c_i} \right)^m \omega^{c_i}, & \text{if } p = 2 \text{ and } m \geq 5,
\end{cases}
\]
and
\[
\delta_s = \begin{cases} 
\left( \frac{-2v}{p} \right)^{m-n} e_{p^{m-n}}, & \text{if } p \text{ is odd,} \\
\left( \frac{2}{v} \right)^{m-n} \omega^v, & \text{if } p = 2 \text{ and } m - n \geq 5,
\end{cases}
\]
and the result is plain when \( p \) is odd or \( p = 2, m - n \geq 5 \).

The remaining cases \( p = 2, m \geq 5 \) and \( m - n = 2, 3, 4 \), follows similarly using the adjustment to \( \delta_s \) observed at the end of the proof of Theorem 2.1.
4. A More Direct Approach

We should note that the Cochrane & Zheng reduction technique [3] can be applied to directly evaluate the Jacobi sums when \( p \) is odd and \( m \geq n + 2 \) instead of the Gauss sums. For example if \( b = p^nb' \) with \( p \nmid b' \), then from [9, Theorem 3.1] we have

\[
J_b(\chi_1, \chi_2, p^m) = \sum_{x=1}^{p^m} \chi_1(x) \chi_2(b - x) = \sum_{x=1}^{p^m} \chi_1 \chi_2(x) \chi_2(bx - 1) = \frac{p^{m+n}}{\chi_1 \chi_2(x_0) \chi_2(bx_0 - 1)} \left( \frac{-2c_2 r b' x_0}{p} \right)^{m-n} \varepsilon_{p^{m-n}},
\]

where \( x_0 \) is a solution to the characteristic equation

\[
c_1 + c_2 - c_1 bx \equiv 0 \mod p^\frac{m+n}{2} + 1, \quad p \nmid x(bx - 1).
\]

If (27) has no solution \( \mod p^\frac{m+n}{2} \) then \( J_b(\chi_1, \chi_2, p^m) = 0 \). In particular we see that:

i. If \( p \nmid c_1 \) and \( p \mid c_2 \), then \( J_b(\chi_1, \chi_2, p^m) = 0 \).

ii. If \( p \nmid c_1 c_2 (c_1 + c_2) \) then

\[
J_b(\chi_1, \chi_2, p^m) = \chi_1 \chi_2(b) \chi_1(\chi_2(c_2) \chi_1 \chi_2(c_1 + c_2) p^{-2} \delta_2.
\]

where

\[
\delta_2 = \left( \frac{-2r}{p} \right)^m \left( \frac{c_1 c_2 (c_1 + c_2)}{p} \right)^m \varepsilon_{p^m}.
\]

iii. If \( p \mid c_1 \) and \( b = p^nb' \), \( p \mid b' \) with \( n < m - 1 \) then \( J_b(\chi_1, \chi_2, p^m) = 0 \) unless \( p^m \mid (c_1 + c_2) \) in which case writing \( w = (c_1 + c_2)/p^m \),

\[
J_b(\chi_1, \chi_2, p^m) = \chi_1 \chi_2(b) \chi_1(\chi_2(c_2) \chi_1 \chi_2(w) \chi_1 \chi_2(b - x_0) = \left( \frac{-2r}{p} \right)^m \left( \frac{c_1 c_2 w}{p} \right)^m \varepsilon_{p^{m-n}}.
\]

To see (ii) observe that if \( p \mid b \), then \( J_b(\chi_1, \chi_2, p^m) = 0 \), and if \( p \nmid b \), then we can take \( x_0 \equiv (c_1 + c_2) c_1^{-1} b^{-1} \mod p^m \) (and hence \( bx_0 - 1 = c_2 c_1^{-1} \)). Similarly for (iii) if \( p^m \mid (c_1 + c_2) \) we can take \( x_0 \equiv -n(c_1 + c_2) c_1^{-1} (b)^{-1} \mod p^m \).

Of course we can write the generalized sum in the form

\[
J_p^n(\chi_1, \ldots, \chi_k) = \sum_{x_3=1}^{p^n} \cdots \sum_{x_k=1}^{p^n} \chi_3(x_3) \ldots \chi_k(x_k) \sum_{b=1}^{p^n-x_3-\cdots-x_k} \chi_1(x_1) \chi_2(b - x_1) \chi_3(x_3) \ldots \chi_k(x_k) J_b(\chi_1, \chi_2, p^m),
\]

Hence assuming that at least one of the \( \chi_i \) is primitive mod \( p^n \) (and reordering the characters as necessary) we see from (i) that \( J_p^n(\chi_1, \ldots, \chi_k, p^m) = 0 \) unless all the characters are primitive mod \( p^n \). Also when \( k = 2, \chi_1, \chi_2 \) primitive, we see from (iii) that \( J_p^n(\chi_1, \chi_2, p^m) = 0 \) unless \( \chi_1 \chi_2 \) is induced by a primitive mod \( p^{m-n} \) character, in which case we recover the formula in Theorem 1.1 on observing that \( \left( \frac{c_1 c_2}{p} \right)^n e_{p^{m-n}}^2 = e_{p^m}^2 \); this is plain when \( n \) is even, for \( n \) odd observe that \( \left( \frac{c_1 c_2}{p} \right) = \left( \frac{c_1 + c_2}{p} \right)^{p-1} \left( \frac{c_1 - c_2}{p} \right) = \left( \frac{-1}{p} \right) \). We show that a simple induction recovers the formula for all \( k \geq 3 \). We assume that all the \( \chi_i \) are primitive mod \( p^n \) and
observe that when \( k \geq 3 \) we can further assume (reordering as necessary) that \( \chi_1 \chi_2 \) is also primitive mod \( p^m \), since if \( \chi_1 \chi_3, \chi_2 \chi_3 \) are not primitive then \( p \mid (c_1 + c_3) \) and \( p \mid (c_2 + c_3) \) and \( (c_1 + c_2) \equiv -2c_3 \neq 0 \mod p \) and \( \chi_1 \chi_2 \) is primitive. Hence from (ii) we can write

\[
J_{p^m}(\chi_1, \ldots, \chi_k, p^m) = \frac{\chi_1(c_1) \chi_2(c_2)}{\chi_1 \chi_2(c_1 + c_2)} p^{\frac{m}{2}} \prod_{x_3 = 1}^{p^m} \chi_3(x_3) \cdots \chi_k(x_k) \chi_1 \chi_2(b) = \chi_1(c_1) \chi_2(c_2) p^{\frac{m}{2}} \prod_{x_a = 1}^{p^m} \chi_3(x_3) \cdots \chi_k(x_k) \chi_1 \chi_2(b)
\]

Assuming the result for \( k - 1 \) characters we have \( J_{p^n}(\chi_1 \chi_2, \chi_3, \ldots, \chi_k, p^m) = 0 \) unless \( \chi_1 \cdots \chi_k \) is induced by a primitive mod \( p^{m-n} \) character in which case

\[
J_{p^n}(\chi_1 \chi_2, \chi_3, \ldots, \chi_k, p^m) = \chi_1 \chi_2(c_1 + c_2) \prod_{i=3}^{k} \chi_i(c_i) \chi_1 \chi_2(v) \delta_3 p^{m(k-2) + n}
\]

with

\[
\delta_3 = \left( \frac{-2r}{p} \right) m(k-2) + n \left( \frac{v}{p} \right) - \left( \frac{c_1 + c_2 + \cdots + c_k}{p} \right) m \left( \frac{k-1}{p} \right) p^{m-n}.
\]

Our formula for \( k \) characters then follows on observing that \( \delta_2 \delta_3 = \delta \).

**References**


