EVALUATING PRIME POWER GAUSS AND JACOBI SUMS

MISTY OSTERGAARD, VINCENT PIGNO AND CHRISTOPHER PINNER

Abstract. We show that for any mod $p^m$ characters, $\chi_1, \ldots, \chi_k$, with at least one $\chi_i$ primitive mod $p^m$, 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 $m \geq 2$ that differs slightly from existing evaluations when $p = 2$.

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. [13, 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 $q = p^m$.

Received April 27, 2016, accepted October 19, 2016.

2010 Mathematics Subject Classification. Primary: 11L05; Secondary: 11L03, 11L10.

Key words and phrases. Gauss sums, Jacobi sums, character sums, exponential sums.

Corresponding author: Vincent Pigno.
Zhang & Yao [12] 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 two of the authors [9] showed that techniques of Cochrane & Zheng [3] (see also [2]) can be used to obtain an evaluation of (1) for any \( m > 1 \) with \( p \) an odd prime. Zhang & Xu [13] considered the general case, (2), and assuming that \( \chi, \chi^{n_1}, \ldots, \chi^{n_k} \), and \( \chi^{n_1 + \cdots + n_k} \) are primitive characters modulo \( p^m \), obtained

\[
J(\chi^{n_1}, \ldots, \chi^{n_k}, p^m) = p^{\frac{k}{2}n_1, \ldots, n_k} \sum_{u=1}^{p^m} \chi(n_1 \cdots n_k), \quad u := n_1 + \cdots + n_k,
\]

(3)

when \( m \) is even, and

\[
J(\chi^{n_1}, \ldots, \chi^{n_k}, p^m) = p^{\frac{k}{2}(k-1)m} \sum_{u=1}^{p^m} \chi(n_1 \cdots n_k) \left\{ \frac{\epsilon_{p}^{-1} \left( \frac{u_1, \ldots, u_k}{p} \right)}{\epsilon_{\frac{2}{p} \frac{u_1, \ldots, u_k}}^{2}} \right\} \quad \text{if } p \neq 2;
\]

(4)

when \( m, k, n_1, \ldots, n_k \) are all odd, where \( \left( \frac{m}{n} \right) \) is the Jacobi symbol and (defined more generally for later use)

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

(5)

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

\[
J_B(\chi_1, \ldots, \chi_k, p^m) = \sum_{x_1, \ldots, x_k \equiv B \mod p^m} \chi_1(x_1) \cdots \chi_k(x_k).
\]

Of course when \( B = p^n B', p \nmid B' \) the simple change of variables \( x_i \rightarrow B' x_i \) gives

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

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 \( x_i \rightarrow -x_k x_i, 1 \leq i < k \) 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 \( n < m \).

For \( p \) odd let \( a \) be a primitive root mod \( p^s \) for all \( s \). We define the integer \( r \) by

\[
a^{\phi(p)} = 1 + r p, \quad p \nmid r.
\]

(6)

For a character \( \chi_i \mod p^m \) we define the integer \( c_i \) by

\[
\chi_i(a) = e_{\phi(p^m)}(c_i), \quad 1 \leq c_i \leq \phi(p^m).
\]

(7)
Note, \( p \nmid c_i \) exactly when \( \chi_i \) is primitive. For \( p = 2, m = 2 \) we take \( a = -1 \) in (7).

For \( p = 2 \) and \( m \geq 3 \) we need two generators \(-1\) and \( 5 \) for \( \mathbb{Z}_{2^m}^* \) and define \( c_i \) by

\[
\chi_i(5) = e^{2^{m-2} c_i}, \quad 1 \leq c_i \leq 2^{m-2}, \tag{8}
\]

with \( \chi_i \) primitive exactly when \( 2 \nmid c_i \).

**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 \( \chi_1, \ldots, \chi_k \) 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 \( J_{p^n}(\chi_1, \ldots, \chi_k, p^m) = 0 \).

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

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

where for \( p \) odd

\[
\delta = \left( \frac{-2r}{p} \right)^{m(k-1)+n} \left( \frac{\nu}{p} \right)^{m-n} \left( \frac{c_1 \cdots c_k}{p} \right)^m \epsilon_p^{m} \epsilon_p^{-1},
\]

with an extra factor \( e^{2\pi i r / 3} \) needed when \( p = m - n = 3, n > 0 \), and for \( p = 2 \) and \( m - n \geq 5 \),

\[
\delta = \left( \frac{2}{v} \right)^{m-n} \left( \frac{2}{c_1 \cdots c_k} \right)^m \omega^{(2^n-1)v}, \tag{10}
\]

with \( \epsilon_p \) as defined in (5), the \( r \) and \( c_i \) as in (6) and (7) or (8), and

\[
v := p^{-m}(c_1 + \cdots + c_k), \quad \omega := e^{\pi i / 4}.
\]

For \( m \geq 5 \) and \( m - n = 2,3 \) or \( 4 \) the formula (10) for \( \delta \) should be multiplied by \( \omega, \omega^{1+\chi_1 \cdots \chi_k(-1)} \), or \( \chi_1 \cdots \chi_k(-1) \omega^{2v} \) 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

\[
J(\chi_1, \ldots, \chi_k, p^m) = p^{\frac{m(k-1)}{2}} \frac{\chi_1(1) \cdots \chi_k(c_k)}{\chi_1 \cdots \chi_k(v)} \delta, \quad v = c_1 + \cdots + c_k,
\]

with

\[
\delta = \begin{cases} 
1, & \text{if } m \text{ is even}, \\
\left( \frac{\nu c_1 \cdots c_k}{p} \right) \left( \frac{-2r}{p} \right)^{k-1} \epsilon_p^{k-1}, & \text{if } m \text{ is odd and } p \neq 2, \\
\left( \frac{2}{\nu c_1 \cdots c_k} \right), & \text{if } m \geq 5 \text{ is odd and } p = 2.
\end{cases}
\]
In the remaining \( n = 0 \) case, \( p = 2, m = 3 \) we have \( J(\chi_1, \ldots, \chi_k, 2^3) = 2 \sum (k-1) (-1)^{\frac{k}{2}} \) 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 \( \chi(a) \) as in (7) or (8)), and for \( m \) even we recover the form (3), and for \( m \) odd we recover (4) but with the addition of a factor \( \left( \frac{-2c}{p} \right)^{k-1} \) for \( p \neq 2 \), which of course can be ignored when \( k \) is odd as assumed in [13].

For completeness we observe that in the few remaining \( m \geq n + 2 \) cases, (9) becomes

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

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

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

where \( \chi \) is a mod \( p^m \) character and \( e_y(x) := e^{2\pi i x/y} \). 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, Evans and Williams [1, Theorem 2.1.3 & Theorem 10.3.1] or Lidl and 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 [12, Lemma 3] for \( k = 2 \), and Zhang and Xu [13, Lemma 1] for general \( k \), showed that

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

In Theorem 2.2 we obtain a similar expansion for \( J_{p^m}(\chi_1, \ldots, \chi_k, p^m) \). Wang [11, Theorem 2.5] had in fact already obtained such an expression for Jacobi sums over much more general rings of residues modulo prime powers. (However, we use a slightly different form to avoid splitting into cases as there.) 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 \( m = n + 1 \) and 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 \( |J_{p^m}(\chi_1, \ldots, \chi_k, p^m)| = p\frac{1}{2}(mk-1) \) if \( \chi_1 \cdots \chi_k = \chi_0 \) and \( p\frac{1}{2}(mk-1) \) otherwise, but an explicit evaluation in the latter case is equivalent to an explicit evaluation of the mod \( p \) Gauss sum \( G(\chi_1 \cdots \chi_k, p) \) when \( m \geq 2 \).
2. Gauss sums

In order to use the result from [4] we must establish some congruence relationships. For \( p \) odd let \( a \) be a primitive root mod \( p^m \), \( m \geq 2 \). We define the integers \( R_j, j \geq 1 \), by

\[
a^{\phi(p^j)} = 1 + R_j p^j. \tag{14}
\]

Note that for \( j \geq i \),

\[
R_j \equiv R_i \mod p^i. \tag{15}
\]

For \( p = 2 \) and \( m \geq 3 \) we define the integers \( R_j, j \geq 2 \), by

\[
5^{2^{j-2}} = 1 + R_j 2^j. \tag{16}
\]

Noting that \( R_2^2 \equiv 1 \mod 8 \), we get

\[
R_i + 1 = R_i + 2^{i-1} R_i^2 \equiv R_i + 2^{i-1} \mod 2^{i+2}. \tag{17}
\]

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

\[
R_j \equiv R_{i+2} \equiv R_{i+1} + 2^i \equiv (R_i + 2^{i-1}) + 2^i \equiv R_i - 2^{i-1} \mod 2^{i+1} \tag{18}
\]

and

\[
R_j \equiv (R_{i-1} + 2^{i-2}) - 2^{i-1} \equiv R_{i-1} - 2^{i-2} \mod 2^{i+1}. \tag{19}
\]

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 \( p \) odd this is essentially the same as Cochrane & Zheng [4, §10] but here we use the simpler \( R_j \) as opposed to the \( p \)-adic logarithm used in [4]; an adjustment to their formula is also needed in the case \( p^m = 3^3 \) (see errata for [3]). For \( p = 2 \) we use the same technique to get a new evaluation of the Gauss sum. Variations can be found in Odoni [7] and Mauclaire [6] (see also Berndt & Evans [1, §1.6 ] and Cochrane [2, Theorem 6.1]).

**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

\[
G(\chi, p^m) = p^m \chi \left(-cR_j^{-1}\right) e_{p^m} \left(-cR_j^{-1}\right) \begin{cases} 
\left(\frac{2c}{p}\right)^m, & \text{if } p \neq 2, p^m \neq 27, \\
\left(\frac{2}{c}\right)^m \omega^c, & \text{if } p = 2 \text{ and } m \geq 5,
\end{cases} \tag{20}
\]

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 \( p = 2 \).

When \( p^m = 27 \) an extra factor \( e_3(-rc) \) is needed. For the remaining cases

\[
G(\chi, 2^m) = 2^m \begin{cases} 
i, & \text{if } m = 2, \\
\omega^{1-\chi(-1)}, & \text{if } m = 3, \\
\chi(-c)e_{16}(-c), & \text{if } m = 4.
\end{cases} \tag{21}
\]
Here $x^{-1}$ denotes the inverse of $x$ mod $p^m$, and $r$, $c$ and $R_j$ are as in (6), (7) or (8), and (14) or (16), $\omega$ as in (11), and $\epsilon_p$ as in (5).

**Proof.** When $p$ is odd, $p^m \neq 27$, [8, Theorem 2.1] gives

$$G(\chi, p^m) = p^{m/2} \chi(\alpha)e_{p^m}(\alpha)\left(-\frac{2rc}{p^m}\right)\epsilon_{p^m}$$

where $\alpha$ is a solution of

$$c + R_jx \equiv 0 \mod p^j, \ J := \left\lceil \frac{m}{2} \right\rceil,$$

and $G(\chi, p^m) = 0$ if no solution exists. So, if $p \mid c$, there is no solution and $G(\chi, p^m) = 0$. If, however, $p \nmid c$, by (15) we may take $\alpha = -cR_j^{-1} \equiv -cR_j^{-1} \mod p^j$ for any $j \geq J$. When $p^m = 27$ we need the extra factor $e_3(-rc)$.

If $p = 2$, $m \geq 6$, and $\chi$ is primitive, then [8, Theorem 5.1] gives

$$G(\chi, 2^m) = 2^{m/2} \chi(\alpha)e_{2^m}(\alpha)\begin{cases} 1, & \text{if } m \text{ is even}, \\ 1 + (-1)^{jR_jc}/\sqrt{2}, & \text{if } m \text{ is odd}, \end{cases}$$

where $\alpha$ is a solution to

$$c + R_j\alpha \equiv 0 \mod 2^{\lceil\frac{m}{2}\rceil},$$

and $c + R_j\alpha = 2^{\lceil\frac{m}{2}\rceil}\lambda$. If $\chi$ is imprimitive, then $G(\chi, 2^m) = 0$. If $2 \nmid c$ and $j \geq J + 2$ then, using (18), we can take

$$\alpha \equiv -cR_j^{-1} \equiv -c(R_j + 2^{j-1})^{-1} \equiv -c(R_j^{-1} - 2^{j-1}) \mod 2^{j+1},$$

and

$$\chi(\alpha)e_{2^m}(\alpha) = \chi(-cR_j^{-1})e_{2^m}(-cR_j^{-1})\chi(1 - R_j2^{j-1})e_{2^m}(c2^{j-1}).$$

Checking the four possible $c$ mod 8,

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

Now

$$e_{2^m}(c2^{j-1}) = e_{2^{m-2}}(c2^{j-3}) = \chi(52^{j-3}) = \chi(1 + R_{j-1}2^{j-1}),$$

where, since $R_j \equiv R_{j-1} - 2^{j-2} \mod 2^{j+1}$ and $R_j \equiv -1 \mod 4$,

$$(1 - R_j2^{j-1})(1 + R_{j-1}2^{j-1}) = 1 + (R_{j-1} - R_j)2^{j-1} - R_j R_{j-1}2^{2j-2} \equiv 1 + 2^{2j-3} + R_{j-1}2^{2j-2} \mod 2^m.$$
Noting that \( R_s \equiv -1 \mod 2^3 \) for \( s \geq 4 \) (and checking by hand for \( J = 3 \) or 4) gives \( 1 + 2R_{J-1} \equiv R_{2J-3} \mod 8 \), and

\[
(1 - R_J 2^{J-1}) (1 + R_{J-1} 2^{J-1}) \equiv 1 + R_{2J-3} 2^{2J-3} \mod 2^m.
\]

Hence

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

One can check numerically that the formula still holds for the \( 2^{m-2} \) primitive mod \( 2^m \) characters when \( m = 5 \). For \( m = 2, 3, 4 \), one has (21) instead of \( 2i\omega, 2^3\omega^2, 2^5\chi(c)e_2(c)\omega^c \) (so our formula (20) requires an extra factor \( \omega^{-1}, \omega^{-1-\chi(-1)} \) or \( \chi(-1)\omega^{-2c} \) respectively). \( \square \)

We shall need the counterpart of (13) for \( J_{p^n}(\chi_1, \ldots, \chi_k) \). We now state a less symmetrical version to allow weaker assumptions on the \( \chi_i \).

**Theorem 2.2.** Suppose that \( \chi_1, \ldots, \chi_k \) are mod \( p^m \) characters with at least one of them primitive and that \( m > n \). If \( \chi_1 \cdots \chi_k \) is a mod \( p^{m-n} \) character, then

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

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

Recall the well-known properties of Gauss sums (see for example [1, §1.6]),

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

So 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

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

In particular we recover (13) under the sole assumption that \( \chi_1 \cdots \chi_k \) is a primitive mod \( p^m \) character.

**Proof.** We first note that if \( \chi \) is a primitive character mod \( p^j \), \( j \geq 1 \) and \( A \in \mathbb{Z} \), then

\[
\sum_{y=1}^{p^j} \chi(y)e_{p^j}(Ay) = \overline{\chi}(A)G(\chi, p^j).
\]
Indeed, for \( p \mid A \) 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 \( \chi(z) \neq 1 \). To see this, note that 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

\[
\sum_{y=1}^{p^j} \chi(y)e_{p^j}(Ay) = \sum_{y=1}^{p^j} \chi(zy)e_{p^j}(Azy) = \chi(z) \sum_{y=1}^{p^j} \chi(y)e_{p^j}(Ay)
\]

(27)

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

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

\[
\overline{\chi_k}(-1)G(\overline{\chi_k}, p^m) \prod_{x_i=1}^{p^m} \chi_1(x_1) \cdots \chi_{k-1}(x_{k-1}) \chi_k(p^m - x_1 - \cdots - x_{k-1})
\]

\[
= \overline{\chi_k}(-1) \prod_{x_i=1}^{p^m} \chi_1(x_1) \cdots \chi_{k-1}(x_{k-1}) \chi_k(p^m - x_1 - \cdots - x_{k-1}) Y
\]

\[
= \sum_{y=1}^{p^m} \chi_1(x_1) e_{p^m}(-x_1 y) \cdots \sum_{x_{k-1}=1}^{p^m} \chi_{k-1}(x_{k-1}) e_{p^m}(-x_{k-1} y)
\]

\[
= \sum_{y=1}^{p^m} \chi_1(x_1 e_{p^m}(-x_1 y)) \cdots \sum_{x_{k-1}=1}^{p^m} \chi_{k-1}(x_{k-1} e_{p^m}(-x_{k-1} y))
\]

\[
= \chi_1 \cdots \chi_{k-1}(-1) \prod_{y=1}^{p^m} \chi_1 \cdots \chi_k(y) e_{p^m}(p^m Y) \prod_{i=1}^{k-1} G(\chi_i, p^m).
\]

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

\[
\sum_{y=1}^{p^m} \chi_1 \cdots \chi_k(y) e_{p^m}(p^n Y) = p^n \sum_{y=1}^{p^m-n} \chi_1 \cdots \chi_k(y) e_{p^{m-n}}(y) = p^n G(\chi_1 \cdots \chi_k, p^{m-n}).
\]

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 (27)

\[
\sum_{y=1}^{p^m} \chi_1 \cdots \chi_k(y) e_{p^m}(p^n Y) = p^{m-j} \sum_{y=1}^{p^j} \chi_1 \cdots \chi_k(y) e_{p^j}(p^{j-(m-n)} Y) = 0
\]

and the result follows from observing that \( G(\chi, p^m) = \overline{\chi}(-1)G(\overline{\chi}, p^m) \) and, since \( \chi_k \) is primitive,

\( G(\chi_k, p^m) = p^m G(\chi_k, p^m)^{-1} \).
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 (25), $J_{p^n}(\chi_1, \ldots, \chi_k, p^m) = 0$. In particular we have (26).

We write $R = R_{\left\lfloor \frac{m}{2} \right\rfloor + 2}$, and then by (26) and the evaluation of Gauss sums in Theorem 2.1 we have

$$J_{p^n}(\chi_1, \ldots, \chi_k, p^m) = \frac{\prod_{i=1}^k G(\chi_i, p^m)}{G(\chi_1 \cdots \chi_k, p^{m-n})} = \frac{\prod_{i=1}^k p^{m/2} \chi_i(-c_i R^{-1}) e^{p^{m-n}(-c_i R^{-1})} \delta_i}{p^{(m-n)/2} \chi_1 \cdots \chi_k(-v R^{-1}) e^{p^{m-n}(-v R^{-1})} \delta_s} = p^{k(m(k-1)+n)} \frac{\prod_{i=1}^k \chi_i(c_i)}{\chi_1 \cdots \chi_k(v)} \delta_s^{-1} \prod_{i=1}^k \delta_i,$$

(28)

where, as long as $p^{m-n} \neq 27$ and $p^m \neq 27$,

$$\delta_i = \left\{ \begin{array}{ll} \left(\frac{-2r c_i}{p}\right)^m & \text{if } p \text{ is odd,} \\ \left(\frac{2}{c_i}\right)^m \omega^{c_i} & \text{if } p = 2 \text{ and } m \geq 5, \end{array} \right.$$

and

$$\delta_s = \left\{ \begin{array}{ll} \left(\frac{-2r v}{p}\right)^{m-n} & \text{if } p \text{ is odd,} \\ \left(\frac{2}{v}\right)^{m-n} \omega^v & \text{if } p = 2 \text{ and } m - n \geq 5, \end{array} \right.$$

and the result is plain when $p$ is odd or $p = 2$, $m - n \geq 5$.

For $p^{m-n} = 3^3$, $p^m \neq 3^3$ we get the extra factor $e_3(r v)$ from the Gauss sum in the denominator, for $p^{m-n} = p^m = 3^3$ or $p^{m-n} \neq 3^3$, $p^m = 3^3$ the additional factors needed in the Gauss sums cancel. The remaining cases $p = 2$, $m \geq 5$ and $m - n = 2, 3, 4$ follow 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 in [3] can be applied to directly evaluate the Jacobi sums instead of turning to Gauss sums, via the binomial character sum evaluations of [9] and [10].

CASE A) ODD $p$ AND $m \geq n + 2$.

If $b = p^n b'$ with $p \nmid b'$ and $\chi_2$ is primitive, then from [9, Theorem 3.1] we have

$$J_b(\chi_1, \chi_2, p^m) = \sum_{x=1}^{p^m} \chi_1(x) \chi_2(b-x) = \sum_{x=1}^{p^m} \chi_1 \chi_2(x) \chi_2(bx-1)$$
we see from (i) that
\[ J_{\chi_1, \chi_2}(x_0, x_1, x_2) = 0 \]
Hence assuming that at least one of the \( x_i \) can take the characteristic equation
\[ c_1 + c_2 - c_1 b x \equiv 0 \mod p^{m-n}, \quad p \nmid x(bx - 1). \]

If (29) has no solution mod \( p^{m-n} \), then \( J_{\chi_1, \chi_2}(x_0, x_1, x_2) = 0 \). In particular we see the following.

(i) If \( p \mid c_1 \) and \( p \nmid c_2 \), then \( J_{\chi_1, \chi_2}(x_0, x_1, x_2) = 0 \).

(ii) If \( p \nmid c_1 c_2 (c_1 + c_2) \) then
\[ J_{\chi_1, \chi_2}(x_0, x_1, x_2) = p^{m-n} \chi_1(x_0) \chi_2(b) \chi_1(c_1) \chi_2(c_2) \chi_1(x_1) \chi_2(x_2) \delta_2. \]
where
\[ \delta_2 = \left( \frac{-2r}{p} \right)^m \left( \frac{c_1 c_2 (c_1 + c_2)}{p} \right)^m \varepsilon_{p^{m-n}}. \]

(iii) If \( p \nmid c_1 \) and \( b = p^n b' \), \( p \nmid b' \) with \( n < m - 1 \) then \( J_{\chi_1, \chi_2}(x_0, x_1, x_2) = 0 \) unless \( p^n \mid (c_1 + c_2) \) in which case writing \( w = (c_1 + c_2)/p^n \), we get
\[ J_{\chi_1, \chi_2}(x_0, x_1, x_2) = p^{m-n} \chi_1(x_0) \chi_2(b') \chi_1(c_1) \chi_2(c_2) \chi_1(x_1) \chi_2(w) \left( \frac{-2r}{p} \right)^{m-n} \left( \frac{c_1 c_2 w}{p} \right)^{m-n} \varepsilon_{p^{m-n}}, \]
with an extra factor \( e_3(r w) \) needed when \( p^{m-n} = 27, n > 0 \).

To see (ii) observe that if \( p \mid b \), then \( J_{\chi_1, \chi_2}(x_0, x_1, x_2) = 0 \), and if \( p \nmid b \), then we can take \( x_0 \equiv (c_1 + c_2) c_1^{-1} b^{-1} \mod p^n \) (and hence \( b x_0 - 1 = c_2 c_1^{-1} \)). Similarly for (iii) if \( p^n \mid (c_1 + c_2) \) we can take \( x_0 \equiv p^{-n} (c_1 + c_2) c_1^{-1} (b')^{-1} \mod p^m \).

Of course we can write the generalized sum in the form
\[ J_{p^n}(\chi_1, \ldots, \chi_k, p^m) = \sum_{x_3=1}^{p^m} \cdots \sum_{x_k=1}^{p^m} \chi_3(x_3) \cdots \chi_k(x_k) \sum_{x_1=1}^{p^m} \chi_1(x_1) \chi_2(b - x_1) \]
\[ = \sum_{x_3=1}^{p^m} \cdots \sum_{x_k=1}^{p^m} \chi_3(x_3) \cdots \chi_k(x_k) J_{\chi_1, \chi_2}(x_0, x_1, x_2) f_b(\chi_1, \chi_2, p^m), \]
Hence assuming that at least one of the \( \chi_i \) is primitive mod \( p^m \) (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 \( p^m \). 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 \( \left( \frac{c_1 c_2}{p} \right) \equiv 1 \mod 4 \); this is plain when \( n \) is even, for \( n \) odd observe that \( \left( \frac{c_1 c_2}{p} \right) = \left( \frac{(c_1 + c_2)^2 - (c_1 - c_2)^2}{p} \right) = \left( \frac{-1}{p} \right) \).

We show that a simple induction recovers the formula for all \( k \geq 3 \). We assume that all the \( \chi_i \) are primitive mod \( p^m \) and observe that when \( k \geq 3 \) we can further assume (reordering as necessary) that \( \chi_1 \chi_2 \) is also primitive mod \( p^m \), since if \( \chi_1 \chi_3, \chi_2 \chi_4 \) are not primitive then \( p | (c_1 + c_3) \) and \( p | (c_2 + c_3) \) and \( (c_1 + c_2) \equiv -2c_3 \not\equiv 0 \mod p \) and \( \chi_1 \chi_2 \) is primitive. Hence from (ii) we can write

\[
J_{p^m}(\chi_1, \ldots, \chi_k, p^m) = \frac{\chi_1(c_1)\chi_2(c_2)}{\chi_1\chi_2(c_1 + c_2)} p^2 \delta_2 \sum_{x_1} \sum_{x_1} \chi_3(x_3) \ldots \chi_k(x_k)\chi_1\chi_2(b) = p^2 \chi_1(c_1)\chi_2(c_2) \chi_1\chi_2(c_1 + c_2) \delta_2 J_{p^n}(\chi_1\chi_2, \chi_3, \ldots, \chi_k, p^m).
\]

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

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

where

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

plus an additional factor \( e_3(r v) \) if \( p^{m-n} = 27, n > 0 \). Our formula for \( k \) characters then follows on observing that \( \delta_2 \delta_3 = \delta \).

**CASE B) WHEN** \( p = 2 \) **AND** \( m \geq n + 5 \).

Suppose that \( \chi_2 \) is primitive mod \( 2^m \), that is \( 2 | c_2 \), and \( b = 2^n b' \) with \( 2 | b' \) and \( m \geq n + 5 \). In this case from [10, Theorem 1.1] we similarly have \( J_b(\chi_1, \chi_2) = 0 \) unless \( 2 | c_1 \) and \( 2^n | c_1 + c_2 \), in which case

\[
J_b(\chi_1, \chi_2, 2^m) = 2^{\frac{1}{2}(m+n)} \chi_1\chi_2(x_0)\chi_2(bx_0 - 1) \begin{cases} 
1, & \text{if } m - n \text{ is even,} \\
\omega^h \left( \frac{2}{7} \right), & \text{if } m - n \text{ odd,}
\end{cases}
\]

where \( x_0 \) is a solution to

\[-(c_1 + c_2)(bx_0 - 1) + c_2 bx_0 R_N R_{-1} = 0 \mod 2^{N+n+3},\]

with \( 2 | x_0(bx_0 - 1) \) and

\[
\omega := e_8(1), \quad N := \left[ \frac{1}{2} (m - n) \right] \geq 3, \quad v := \frac{c_1 + c_2}{2^n}, \quad h := -(2^n - 1)v \mod 8.
\]
From the relations (17) we obtain

$$R_{i+n} R_i^{-1} - 1 = 2^{i-1} \mu_i, \quad \mu_i \equiv (2^n - 1) R_i \mod 8,$$

where $R_2 = 1$, $R_3 = 3$, and $R_j \equiv -1 \mod 8$ for $j \geq 4$. Hence, taking

$$x_0 = v b^{r-1} (c_1 + c_2 - c_2 R_N R_{N+n}^{-1})^{-1},$$

we get

$$J_b(\chi_1, \chi_2, 2^m) = 2^{\frac{1}{2}(m+n)} \frac{\chi_1(1 \chi_2(2^m \chi_1(1 \chi_2(v) \left(\frac{2}{v}\right)^{m-n} \epsilon}

with

$$\epsilon := \overline{\chi_2(1 + 2N^{-1} \mu_N)} \chi_1(1 + c_1^{-1} v \mu_N 2^{N+n-1}) \begin{cases} 1, & \text{if } m-n \text{ is even}, \\ \omega^{-(2^n-1)v} \left(\frac{2}{2^{n-1}}\right), & \text{if } m-n \text{ is odd}, \end{cases}$$

where $\overline{\chi_2}$ is a primitive mod $2^{m-n}$ character. Expanding binomially, observing that $2(N + n - 1) \geq m$ if $n \geq 2$ or $m$ is even, and $2(N + n - 1) = m - 1$ if $n = 1$ and $m$ is odd, one readily obtains

$$1 + c_1^{-1} v \mu_N 2^{N+n-1} \equiv (1 + R_{N+n-1} 2^{N+n-1})^x = 5^{2^{N+n-1}} \mod 2^m,$$

with

$$\kappa := c_1^{-1} v \mu_N R_{N+n-1}^{-1} \begin{cases} \frac{1}{2} (v - c_1) 2^{(m-1)/2}, & \text{if } n = 1, m \text{ odd}, \\ 0, & \text{else}. \end{cases}$$

Similarly,

$$1 + 2^{N-1} \mu_N \equiv 1 + R_{N-1} 2^{N-1} \mu_N R_{N-1}^{-1} \equiv 1 + 2^{N-1} R_{N-1} \mu_N R_{N+n-1}^{-1} (1 + 2^{N-2} \mu_{N-1})$$

$$\equiv 1 + R_{N-1} 2^{N-1} \left(\mu_N R_{N+n-1}^{-1} + 2^{N-2} R_N R_{N-1} R_{N+n-1}^{-1}\right) \mod 2^{m-n}$$

and, since $3(N - 1) \geq m - n$,

$$1 + 2^{N-1} \mu_N \equiv (1 + R_{N-1} 2^{N-1})^\mu_N R_{N+n-1}^{-1} 2^{N-2}(2^n-1) = 5^{2^{N-3} (\mu_N R_{N+n-1}^{-1} 2^{N-2}(2^n-1))} \mod 2^{m-n}.$$ 

Hence, checking the possibilities mod 8, recalling that $2^n \parallel c_1 + c_2$,

$$\epsilon = e_{2^{m-n-2N+3}}((2^n - 1)v) \begin{cases} (-1)^{\frac{1}{2}(v-c_1)}, & \text{if } m-n \text{ is even and } n = 1, \\ 1, & \text{if } m-n \text{ is even and } n \geq 2, \\ \omega^{-(2^n-1)v} \left(\frac{2}{2^{n-1}}\right), & \text{if } m-n \text{ odd}. \end{cases}$$

and we obtain the $p = 2, k = 2$ result of Theorem 1.1. As in the case of odd $p$ we can deduce from the $k = 2$ result that $J_b(\chi_1, \ldots, \chi_k, 2^m) = 0$ if the sum contains both primitive and
imprimitive $\chi_i$ mod $2^m$. Hence in the following we assume that all the $\chi_i$ are primitive mod $2^m$.

For $k = 3$ we observe from parity considerations that $J_b(\chi_1, \chi_2, \chi_3, 2^m) = 0$ if $b$ is even, while if $b$ is odd we can make the change of variables $x_i \mapsto bx_i$. Hence in either case

$$J_b(\chi_1, \chi_2, \chi_3, 2^m) = \chi_1 \chi_2 \chi_3(b) J(\chi_1, \chi_2, \chi_3, 2^m). \quad (30)$$

Now at least one of $\chi_1 \chi_2, \chi_1 \chi_3, \chi_2 \chi_3$ is primitive mod $2^{m-1}$ (since they are all mod $2^{m-1}$ characters and $\chi_1^2 = \chi_1 \chi_2 \cdot \chi_1 \chi_3 \cdot \chi_2 \chi_3$ is primitive mod $2^{m-1}$). We suppose that $\chi_1 \chi_2$ is primitive mod $2^{m-1}$, i.e. $2 \parallel c_1 + c_2$. Then

$$J(\chi_1, \chi_2, \chi_3, 2^m) = \sum_{x_3 = 1}^{2^m} \chi_3(x_3) J_{1-x_3}(\chi_1, \chi_2, 2^m)$$

$$= 2^{\frac{1}{2}(m+1)} \frac{\chi_1(c_1) \chi_2(c_2)}{\chi_1 \chi_2} \left( 2 \frac{2}{c_1 + c_2} \right)^{m-1} \sum_{x_3 = 1}^{2^m} \chi_3(x_3) \chi_1 \chi_2 \left( \frac{1-x_3}{2} \right).$$

Now

$$\sum_{x_3 = 1}^{2^m} \chi_3(x_3) \chi_1 \chi_2 \left( \frac{1-x_3}{2} \right) = \frac{1}{2} \sum_{1=x_3=1}^{2^m} \chi_3(x_3) \chi_1 \chi_2(x),$$

which, from the change of variables $x \mapsto x^{-1}$, $x_3 \mapsto -x_3 x^{-1}$ and the $k = 2$ result, equals

$$\frac{1}{2} \chi_3(-1) \sum_{x_3 = 1}^{2^m} \chi_3(x_3) \frac{1}{\chi_1 \chi_2 \chi_3}(x) =$$

$$2^{\frac{1}{2}(m-1)} \chi_3(-1) \frac{\chi_1 \chi_2 \chi_3}{\chi_1 \chi_2} \left( 2 \frac{2}{c_1 + c_2} \right)^{m-1} \left( 2 \frac{c_1 + c_2}{c_1 + c_2 + c_3} \right)^m \omega^{-\frac{1}{2}(c_1 + c_2)},$$

since $\chi_3 \chi_1 \chi_2 \chi_3 = \chi_1 \chi_2$ and $2 \parallel c_i$ ensures that $2 \parallel c_1 + c_2 + c_3$. Hence

$$J(\chi_1, \chi_2, \chi_3, 2^m) = 2^m \frac{\chi_1(c_1) \chi_2(c_2) \chi_3(c_3)}{\chi_1 \chi_2 \chi_3(c_1 + c_2 + c_3)} \left( 2 \frac{2}{c_1 + c_2 + c_3} \right)^m \left( 2 \frac{c_1 + c_2}{c_1 c_2 c_3} \right)^m,$$

and we recover Theorem 1.1 when $k = 3$ (note $J_{b^n}(\chi_1, \chi_2, \chi_3, 2^m) = 0$ unless $n = 0$).

For $k \geq 4$ we use (30) to write

$$J_b(\chi_1, \ldots, \chi_k, 2^m) = J_b(\chi_1 \chi_2 \chi_3, \chi_4, \ldots, \chi_n, 2^m) J(\chi_1, \chi_2, \chi_3, 2^m)$$

and the Theorem 1.1 result for general $k$ follows easily by induction.
References


Department of Mathematics, University of Southern Indiana, Evansville, IN 47712.

E-mail: m.ostergaard@usi.edu

Department of Mathematics & Statistics, California State University, Sacramento, Sacramento, CA 95819.

E-mail: vincent.pigno@csus.edu

Department of Mathematics, Kansas State University, Manhattan, KS 66506.

E-mail: pinner@math.ksu.edu