TAMKANG JOURNAL OF MATHEMATICS
Volume 48, Number 3, 227-240, September 2017
doi:10.5556/j.tkjm.48.2017.1866
This paper is available online at http://journals.math.tku.edu.tw/index.php/TKJM/pages/view/onlinefirst

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 χ_i primitive mod p^m, the Jacobi sum,

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

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

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

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

$$J(\chi_1,\ldots,\chi_k,q)=\sum_{\substack{x_1=1\\ x_1+\cdots+x_k\equiv 1 \bmod q}}^{q}\cdots\sum_{x_k=1}^{q}\chi_1(x_1)\cdots\chi_k(x_k). \tag{2}$$

If the χ_i are mod rs characters with $(r,s)=1$, then, writing $\chi_i=\chi_i'\chi_i''$ where χ_i' and χ_i'' are mod r and mod s characters respectively, 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 χ_1, χ_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 $\chi, \chi^{n_1}, \dots, \chi^{n_k}$, and $\chi^{n_1+\cdots+n_k}$ are primitive characters modulo p^m, obtained

$$J(\chi^{n_1},\dots,\chi^{n_k},p^m) = p^{\frac{1}{2}(k-1)m}\overline{\chi}(u^u)\chi(n_1^{n_1}\dots n_k^{n_k}),\ \ u := n_1+\cdots+n_k, \tag{3}$$

when m is even, and

$$J(\chi^{n_1},\dots,\chi^{n_k},p^m) = p^{\frac{1}{2}(k-1)m}\overline{\chi}(u^u)\chi(n_1^{n_1}\dots n_{k-1}^{n_{k-1}}) \begin{cases} \varepsilon_p^{k-1}\left(\frac{un_1\dots n_k}{p}\right), & \text{if } p \neq 2; \\ \left(\frac{2}{un_1\dots n_k}\right) & \text{if } p = 2, \end{cases} \tag{4}$$

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

$$\varepsilon_{p^m} := \begin{cases} 1, & \text{if } p^m \equiv 1 \bmod 4, \\ i, & \text{if } p^m \equiv 3 \bmod 4. \end{cases} \tag{5}$$

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

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

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

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

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

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

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

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

$$a^{\phi(p)} = 1 + rp, \quad p \nmid r. \tag{6}$$

For a character χ_i mod p^m we define the integer c_i by

$$\chi_i(a) = e_{\phi(p^m)}(c_i), \quad 1 \le c_i \le \phi(p^m). \tag{7}$$

Note, $p \nmid c_i$ exactly when χ_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 χ_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 $\chi_1\ldots\chi_k$ 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

$$J_{p^n}(\chi_1,\ldots,\chi_k,p^m)=p^{\frac{1}{2}(m(k-1)+n)}\frac{\chi_1(c_1)\cdots\chi_k(c_k)}{\chi_1\cdots\chi_k(v)}\delta, \tag{9}$$

where for p odd

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

with an extra factor $e^{2\pi irv/3}$ 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 ε_{p^m} as defined in (5), the r and c_i as in (6) and (7) or (8), and

$$v:=p^{-n}(c_1+\cdots+c_k), \quad \omega:=e^{\pi i/4}. \tag{11}$$

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

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

with

$$\delta=\begin{cases}1, & \text{if } m \text{ is even,}\\ \left(\frac{vc_1\cdots c_k}{p}\right)\left(\frac{-2r}{p}\right)^{k-1}\varepsilon_p^{k-1}, & \text{if } m \text{ is odd and } p\neq 2,\\ \left(\frac{2}{vc_1\cdots c_k}\right), & \text{if } m\geq 5 \text{ is odd and } p=2.\end{cases}$$

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

When the $\chi_i=\chi^{n_i}$ for some primitive mod p^m character χ, we can write $c_i=n_ic$ (where c is determined by $\chi(a)$ as in (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 $\left(\frac{-2rc}{p}\right)^{k-1}$ 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

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

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

$$G(\chi,p^m):=\sum_{x=1}^{p^m}\chi(x)e_{p^m}(x), \tag{12}$$

where χ is a mod p^m character and $e_y(x):=e^{2\pi ix/y}$. 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 $\chi_1,\dots,\chi_k$, 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

$$J(\chi_1,\dots,\chi_k,p^m)=\frac{\prod_{i=1}^k G(\chi_i,p^m)}{G(\chi_1\dots\chi_k,p^m)}. \tag{13}$$

In Theorem 2.2 we obtain a similar expansion for $J_{p^n}(\chi_1,\dots,\chi_k,p^m)$. 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 χ_i primitive, the Jacobi sum is still zero unless all the χ_i are primitive mod p^m and $\chi_1\cdots\chi_k$ is a mod p character. Then we can say that $|J_{p^n}(\chi_1,\dots,\chi_k,p^m)|$ $=p^{\frac{1}{2}mk-1}$ if $\chi_1\cdots\chi_k=\chi_0$ and $p^{\frac{1}{2}(mk-1)}$ otherwise, but an explicit evaluation in the latter case is equivalent to an explicit evaluation of the mod p Gauss sum $G(\chi_1\cdots\chi_k,p)$ when $m\geq 2$.

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 $j \geq i$,

$$R_j \equiv R_i \bmod p^i. \tag{15}$$

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 $R_i^2 \equiv 1 \bmod 8$, we get

$$R_{i+1} = R_i + 2^{i-1} R_i^2 \equiv R_i + 2^{i-1} \bmod 2^{i+2}. \tag{17}$$

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

$$R_j \equiv R_{i+2} \equiv R_{i+1} + 2^i \equiv (R_i + 2^{i-1}) + 2^i \equiv R_i - 2^{i-1} \bmod 2^{i+1} \tag{18}$$

and

$$R_j \equiv (R_{i-1} + 2^{i-2}) - 2^{i-1} \equiv R_{i-1} - 2^{i-2} \bmod 2^{i+1}. \tag{19}$$

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

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

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

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

$$G(\chi, 2^m) = 2^{\frac{m}{2}} \begin{cases} i, & \text{if } m = 2, \\ \omega^{1-\chi(-1)}, & \text{if } m = 3, \\ \chi(-c) e_{16}(-c), & \text{if } m = 4. \end{cases} \tag{21}$$

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), ω as in (11), and ε_{p^m} as in (5).

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

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

where α is a solution of

$$c + R_J x \equiv 0 \bmod p^J, \quad J := \left\lceil \frac{m}{2} \right\rceil, \tag{22}$$

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 $\alpha = -cR_J^{-1} \equiv -cR_j^{-1} \bmod p^J$ for any $j \geq J$. When $p^m = 27$ we need the extra factor $e_3(-rc)$.

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

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

where α is a solution to

$$c + R_J x \equiv 0 \bmod 2^{\lfloor \frac{m}{2} \rfloor}, \tag{23}$$

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

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

and

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

Checking the four possible c mod 8,

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

Now

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

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

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

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

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

Hence

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

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

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 χ_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*

$$J_{p^n}(\chi_1, \ldots, \chi_k, p^m) = p^{-(m-n)} \overline{G(\chi_1 \cdots \chi_k, p^{m-n})} \prod_{i=1}^{k} G(\chi_i, p^m). \tag{24}$$

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]),

$$|G(\chi, p^j)| = \begin{cases} p^{j/2}, & \text{if } \chi \text{ is primitive mod } p^j, \\ 1, & \text{if } \chi = \chi_0 \text{ and } j = 1, \\ 0, & \text{otherwise.} \end{cases} \tag{25}$$

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

$$J_{p^n}(\chi_1, \ldots, \chi_k, p^m) = \frac{\prod_{i=1}^{k} G(\chi_i, p^m)}{G(\chi_1 \ldots \chi_k, p^{m-n})}. \tag{26}$$

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

$$\sum_{y=1}^{p^j} \chi(y) e_{p^j}(Ay) = \sum_{y=1}^{p^j} \chi(zy) e_{p^j}(Azy) = \chi(z) \sum_{y=1}^{p^j} \chi(y) e_{p^j}(Ay) \tag{27}$$

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

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

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

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

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

If $\overline{\chi_1 \ldots \chi_k}$ is a primitive character mod p^j with $m - n < j \leq m$, then by the same reasoning as in (27)

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

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

3. Proof of Theorem 1.1

We assume that $\chi_1,\dots,\chi_k$ are all primitive mod p^m characters and $\chi_1\cdots\chi_k$ is a primitive mod p^{m-n} character, since otherwise from Theorem 2.2 and (25), $J_{p^n}(\chi_1,\dots,\chi_k,p^m)=0$. In particular we have (26).

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

$$\begin{aligned} J_{p^n}(\chi_1,\dots,\chi_k,p^m) &= \frac{\prod_{i=1}^k G(\chi_i,p^m)}{G(\chi_1\dots\chi_k,p^{m-n})}\\ &= \frac{\prod_{i=1}^k p^{m/2}\chi_i(-c_iR^{-1})e_{p^m}(-c_iR^{-1})\delta_i}{p^{(m-n)/2}\chi_1\dots\chi_k(-vR^{-1})e_{p^{m-n}}(-vR^{-1})\delta_s}\\ &= p^{\frac{1}{2}(m(k-1)+n)}\frac{\prod_{i=1}^k\chi_i(c_i)}{\chi_1\dots\chi_k(v)}\delta_s^{-1}\prod_{i=1}^k\delta_i, \end{aligned} \tag{28}$$

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

$$\delta_i=\begin{cases}\left(\frac{-2rc_i}{p}\right)^m\varepsilon_{p^m}, & \text{if } p \text{ is odd},\\ \left(\frac{2}{c_i}\right)^m\omega^{c_i}, & \text{if } p=2 \text{ and } m\ge 5,\end{cases}$$

and

$$\delta_s=\begin{cases}\left(\frac{-2rv}{p}\right)^{m-n}\varepsilon_{p^{m-n}}, & \text{if } p \text{ is odd},\\ \left(\frac{2}{v}\right)^{m-n}\omega^{v}, & \text{if } p=2 \text{ and } m-n\ge 5,\end{cases}$$

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

For $p^{m-n}=3^3$, $p^m\neq 3^3$ we get the extra factor $e_3(rv)$ 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 $p=2$, $m\ge 5$ and $m-n=2,3,4$ follow similarly using the adjustment to δ_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 $m\ge n+2$.

If $b=p^nb'$ with $p\nmid b'$ and χ_2 is primitive, then from [9, Theorem 3.1] we have

$$J_b(\chi_1,\chi_2,p^m)=\sum_{x=1}^{p^m}\chi_1(x)\chi_2(b-x)=\sum_{x=1}^{p^m}\overline{\chi_1\chi_2}(x)\chi_2(bx-1)$$

$$= p^{\frac{m+n}{2}} \overline{\chi_1\chi_2}(x_0)\chi_2(bx_0-1)\left(\frac{-2c_2rb'x_0}{p}\right)^{m-n} \varepsilon_{p^{m-n}},$$

with an extra factor $e_3(r(c_1+c_2)/p^n)$ needed when $p^{m-n}=27$, $n>0$, where x_0 is a solution to the characteristic equation

$$c_1+c_2-c_1bx \equiv 0 \bmod p^{\lfloor\frac{m+n}{2}\rfloor+1}, \quad p\nmid x(bx-1). \tag{29}$$

If (29) has no solution mod $p^{\lfloor\frac{m+n}{2}\rfloor}$, then $J_b(\chi_1,\chi_2,p^m)=0$. In particular we see the following.

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

(ii) If $p\nmid c_1c_2(c_1+c_2)$ then

$$J_b(\chi_1,\chi_2,p^m) = p^{\frac{m}{2}}\chi_1\chi_2(b)\chi_1(c_1)\chi_2(c_2)\overline{\chi_1\chi_2}(c_1+c_2)\delta_2.$$

where

$$\delta_2 = \left(\frac{-2r}{p}\right)^m \left(\frac{c_1c_2(c_1+c_2)}{p}\right)^m \varepsilon_{p^m}.$$

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

$$J_b(\chi_1,\chi_2,p^m) = p^{\frac{m+n}{2}}\chi_1\chi_2(b')\frac{\chi_1(c_1)\chi_2(c_2)}{\chi_1\chi_2(w)}\left(\frac{-2r}{p}\right)^{m-n}\left(\frac{c_1c_2w}{p}\right)^{m-n}\varepsilon_{p^{m-n}},$$

with an extra factor $e_3(rw)$ needed when $p^{m-n}=27$, $n>0$.

To see (ii) observe that if $p\mid b$, then $J_b(\chi_1,\chi_2,p^m)=0$, and if $p\nmid b$, then we can take $x_0\equiv(c_1+c_2)c_1^{-1}b^{-1} \bmod p^m$ (and hence $bx_0-1=c_2c_1^{-1}$). Similarly for (iii) if $p^n \,\|\, (c_1+c_2)$ we can take $x_0\equiv p^{-n}(c_1+c_2)c_1^{-1}(b')^{-1} \bmod p^m$.

Of course we can write the generalized sum in the form

$$J_{p^n}(\chi_1,\dots,\chi_k,p^m) = \sum_{x_3=1}^{p^m}\cdots\sum_{x_k=1}^{p^m}\chi_3(x_3)\dots\chi_k(x_k)\sum_{\substack{x_1=1\\ b:=p^n-x_3-\cdots-x_k}}^{p^m}\chi_1(x_1)\chi_2(b-x_1)$$
$$= \sum_{x_3=1}^{p^m}\cdots\sum_{x_k=1}^{p^m}\chi_3(x_3)\dots\chi_k(x_k)J_b(\chi_1,\chi_2,p^m),$$

Hence assuming that at least one of the χ_i is primitive mod p^m (and reordering the characters as necessary) we see from (i) that $J_{p^n}(\chi_1,\dots,\chi_k,p^m)=0$ unless all the characters are primitive mod p^m. Also when $k=2$, χ_1,χ_2 primitive, we see from (iii) that $J_{p^n}(\chi_1,\chi_2,p^m)=0$ unless $\chi_1\chi_2$ is induced by a primitive mod p^{m-n} character, in which case we recover the formula in Theorem 1.1 on observing that $\left(\frac{c_1c_2}{p}\right)^n \varepsilon_{p^{m-n}}^2 = \varepsilon_{p^m}^2$; this is plain when n is even, for n odd observe that $\left(\frac{c_1c_2}{p}\right) = \left(\frac{(c_1+c_2)^2-(c_1-c_2)^2}{p}\right) = \left(\frac{-1}{p}\right)$.

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

$$\begin{aligned} J_{p^m}(\chi_1,\ldots,\chi_k,p^m) &= \frac{\chi_1(c_1)\chi_2(c_2)}{\chi_1\chi_2(c_1+c_2)} p^{\frac{m}{2}} \delta_2 \sum_{x_3=1}^{p^m} \cdots \sum_{x_k=1}^{p^m} \chi_3(x_3)\ldots\chi_k(x_k)\chi_1\chi_2(b) \\ &= p^{\frac{m}{2}} \chi_1(c_1)\chi_2(c_2)\overline{\chi_1\chi_2}(c_1+c_2)\delta_2 J_{p^n}(\chi_1\chi_2,\chi_3,\ldots,\chi_k,p^m). \end{aligned}$$

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

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

where

$$\delta_3 = \left(\frac{-2r}{p}\right)^{m(k-2)+n} \left(\frac{v}{p}\right)^{m-n} \left(\frac{(c_1+c_2)c_3\ldots c_k}{p}\right)^m \varepsilon_{p^m}^{k-1}\varepsilon_{p^{m-n}}^{-1},$$

plus an additional factor $e_3(rv)$ 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 χ_2 is primitive mod 2^m, that is $2 \nmid c_2$, and $b = 2^n b'$ with $2 \nmid b'$ and $m \geq n+5$. In this case from [10, Theorem 1.1] we similarly have $J_b(\chi_1,\chi_2) = 0$ unless $2 \nmid c_1$ and $2^n \parallel c_1+c_2$, in which case

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

where x_0 is a solution to

$$-(c_1+c_2)(bx_0-1) + c_2bx_0R_NR_{N+n}^{-1} \equiv 0 \bmod 2^{N+n+3},$$

with $2 \nmid x_0(bx_0-1)$ and

$$\omega := e_8(1),\ \ N := \left\lceil \frac{1}{2}(m-n) \right\rceil \geq 3,\ \ v := \frac{c_1+c_2}{2^n},\ \ h :\equiv -(2^n-1)v \bmod 8.$$

From the relations (17) we obtain

$$R_{l+n}R_l^{-1}-1=2^{l-1}\mu_l,\ \ \mu_l\equiv(2^n-1)R_l \bmod 8,$$

where $R_2=1$, $R_3=3$, and $R_j\equiv -1 \bmod 8$ for $j\geq 4$. Hence, taking $x_0=vb'^{-1}(c_1+c_2-c_2R_NR_{N+n}^{-1})^{-1}$, we get

$$J_b(\chi_1,\chi_2,2^m)=2^{\frac{1}{2}(m+n)}\chi_1\chi_2(b')\frac{\chi_1(c_1)\chi_2(c_2)}{\chi_1\chi_2(v)}\left(\frac{2}{v}\right)^{m-n}\epsilon$$

with

$$\epsilon:=\overline{\chi_1\chi_2}(1+2^{N-1}\mu_N)\chi_1(1+c_1^{-1}v\mu_N2^{N+n-1})\begin{cases}1, & \text{if } m-n \text{ is even,}\\ \omega^{-(2^n-1)v}\left(\frac{2}{2^n-1}\right), & \text{if } m-n \text{ is odd,}\end{cases}$$

where $\overline{\chi_1\chi_2}$ 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

$$1+c_1^{-1}v\mu_N2^{N+n-1}\equiv(1+R_{N+n-1}2^{N+n-1})^{\kappa}=5^{2^{N+n-3}\kappa} \bmod 2^m,$$

with

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

Similarly,

$$\begin{aligned}1+2^{N-1}\mu_N&\equiv 1+R_{N-1}2^{N-1}\mu_NR_{N-1}^{-1}\equiv 1+2^{N-1}R_{N-1}\mu_NR_{N+n-1}^{-1}(1+2^{N-2}\mu_{N-1})\\ &\equiv 1+R_{N-1}2^{N-1}\left(\mu_NR_{N+n-1}^{-1}+2^{N-2}R_NR_{N-1}R_{N+n-1}^{-1}\right) \bmod 2^{m-n}\end{aligned}$$

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

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

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

$$\begin{aligned}\epsilon&=e_{2^{m-n-2N+3}}((2^n-1)v)\cdot\begin{cases}(-1)^{\frac{1}{2}(v-c_1)}, & \text{if } m-n \text{ is even and } n=1,\\ 1, & \text{if } m-n \text{ is even and } n\geq 2,\\ \omega^{-(2^n-1)v}\left(\frac{2}{2^n-1}\right), & \text{if } m-n \text{ odd.}\end{cases}\\ &=\omega^{(2^n-1)v}\left(\frac{2}{c_1c_2}\right)^m\end{aligned}$$

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 $J_b(\chi_1,\dots,\chi_k,2^m)=0$ if the sum contains both primitive and imprimitive χ_i mod 2^m. Hence in the following we assume that all the χ_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

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

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 $\chi_1^2=\chi_1\chi_2\cdot\chi_1\chi_3\cdot\overline{\chi_2\chi_3}$ is primitive mod 2^{m-1}). We suppose that $\chi_1\chi_2$ is primitive mod 2^{m-1}, i.e. $2 \,||\, c_1+c_2$. Then

$$\begin{aligned}J(\chi_1,\chi_2,\chi_3,2^m) &= \sum_{\substack{x_3=1\\ x_3\text{odd}}}^{2^m} \chi_3(x_3)J_{1-x_3}(\chi_1,\chi_2,2^m)\\ &= 2^{\frac{1}{2}(m+1)}\frac{\chi_1(c_1)\chi_2(c_2)}{\chi_1\chi_2\left(\frac{c_1+c_2}{2}\right)}\left(\frac{2}{\frac{c_1+c_2}{2}}\right)^{m-1}\left(\frac{2}{c_1c_2}\right)^m \omega^{\frac{1}{2}(c_1+c_2)}\sum_{\substack{x_3=1\\ x_3\text{odd}}}^{2^m}\chi_3(x_3)\chi_1\chi_2\left(\frac{1-x_3}{2}\right).\end{aligned}$$

Now

$$\sum_{\substack{x_3=1\\ x_3\text{odd}}}^{2^m}\chi_3(x_3)\chi_1\chi_2\left(\frac{1-x_3}{2}\right)=\frac{1}{2}\sum_{\substack{x_3=1\\ 1-x_3\equiv 2x \bmod 2^m}}^{2^m}\sum_{x=1}^{2^m}\chi_3(x_3)\chi_1\chi_2(x)$$

which, from the change of variables $x\mapsto x^{-1}$, $x_3\mapsto -x_3x^{-1}$ and the $k=2$ result, equals

$$\frac{1}{2}\chi_3(-1)\sum_{\substack{x_3=1\\ x+x_3\equiv 2 \bmod 2^m}}^{2^m}\sum_{x=1}^{2^m}\chi_3(x_3)\overline{\chi_1\chi_2\chi_3}(x)=$$

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

since $\chi_3\overline{\chi_1\chi_2\chi_3}=\overline{\chi_1\chi_2}$ and $2\nmid c_i$ ensures that $2\nmid c_1+c_2+c_3$. Hence

$$J(\chi_1,\chi_2,\chi_3,2^m)=2^m\frac{\chi_1(c_1)\chi_2(c_2)\chi_3(c_3)}{\chi_1\chi_2\chi_3(c_1+c_2+c_3)}\left(\frac{2}{c_1+c_2+c_3}\right)^m\left(\frac{2}{c_1c_2c_3}\right)^m,$$

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

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

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

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

References

[1] B.C. Berndt, R.J. Evans and K. S. Williams, *Gauss and Jacobi Sums*, Canadian Math. Soc. series of monographs and advanced texts, vol. 21, Wiley, New York 1998.

[2] T. Cochrane, *Exponential sums modulo prime powers*, Acta Arith., **101** (2002), no. 2, 131–149.

[3] T. Cochrane and Z. Zheng, *Pure and mixed exponential sums*, Acta Arith., **91** (1999), no. 3, 249-278 (for errata see http://www.math.ksu.edu/~ cochrane/research/research09.html).

[4] T. Cochrane and Z. Zheng, *A survey on pure and mixed exponential sums modulo prime powers*, Number theory for the millennium, I (Urbana, IL, 2000), 273-300, A K Peters, Natick,MA, 2002.

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

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

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

[8] V. Pigno and C. Pinner, *Twisted monomial Gauss sums modulo prime powers*, Func. Approx. Comment. Math., **51** (2014), no. 2, 285–301.

[9] V. Pigno and C. Pinner, *Binomial character sums modulo prime powers*, J. Théor. Nombres Bordeaux, **28** (2016), no. 1, 39–53.

[10] V. Pigno, C. Pinner and J. Sheppard, *Evaluating binomial character sums modulo powers of two*, J. Math. Res. Appl., **35** (2015), no. 2, 137–142.

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

[12] W. Zhang and W. Yao, *A note on the Dirichlet characters of polynomials*, Acta Arith., **115** (2004), no. 3, 225–229.

[13] W. Zhang and Z. Xu, *On the Dirichlet characters of polynomials in several variables*, Acta Arith., **121** (2006), no. 2, 117–124.

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