Functiones et Approximatio
56.1 (2017), 49–60
doi: 10.7169/facm/1590

JACOBI-TYPE SUMS WITH AN EXPLICIT EVALUATION MODULO PRIME POWERS

Badria Alsulmi, Vincent Pigno, Christopher Pinner

Abstract: We show that for Dirichlet characters $\chi_1, \dots, \chi_s$ mod p^m the sum

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

has a simple evaluation when m is sufficiently large.

Keywords: character sums, Gauss sums, Jacobi sums.

1. Introduction

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

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

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

$$J_B(\chi_1, \dots, \chi_s, q) := \sum_{\substack{x_1=1 \\ x_1+\cdots+x_s\equiv B \bmod q}}^{q} \cdots \sum_{x_s=1}^{q} \chi_1(x_1)\cdots\chi_s(x_s). \tag{2}$$

A thorough discussion of mod p Jacobi sums and their extension to finite fields can be found in Berndt, R.J. Evans and K. S. Williams [1]. W. Zhang and W. Yao [7] showed that the sums (1) have an explicit evaluation when q is a perfect square

The second author acknowledges support of California State University, Sacramento's Provost's Research Incentive Fund.

2010 Mathematics Subject Classification: primary: 11L10, 11L40; secondary: 11L03,11L05 and Zhang & Xu [8] obtained an evaluation of the sums (2) for certain classes of squareful q (if $p \mid q$, then $p^2 \mid q$) in the classic $B = 1$ case. In [3] Long, Pigno & Pinner extended this to more general squareful q and general B, essentially using reduction techniques of Cochrane & Zheng [2].

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

$$J_B(\vec{\chi}, h, q) := \sum_{\substack{x_1=1 \\ h(x_1,\ldots,x_s) \equiv B \bmod q}}^{q} \cdots \sum_{x_s=1}^{q} \chi_1(x_1) \cdots \chi_s(x_s). \tag{3}$$

As demonstrated in Lemma 5.2 one can usually reduce such sums to the case that $q = p^m$ is a prime power. In this paper we will be concerned with h of the form

$$h(x_1, \ldots, x_s) = A_1 x_1^{k_1} + \cdots + A_s x_s^{k_s}, \qquad p \nmid A_1 \cdots A_s, \tag{4}$$

where the k_i are non-zero integers, and

$$J_B(\vec{\chi}, h, p^m) = \sum_{\substack{x_1=1 \\ A_1 x_1^{k_1} + \cdots + A_s x_s^{k_s} \equiv B \bmod p^m}}^{p^m} \cdots \sum_{x_s=1}^{p^m} \chi_1(x_1) \cdots \chi_s(x_s). \tag{5}$$

As well as (2) this generalization includes the binomial character sums

$$\sum_{x=1}^{p^m} \chi_1(x) \chi_2(Ax^k + B), \tag{6}$$

shown to also have an explicit evaluation in [5, Theorem 3.1]. A different generalization of these sums having an explicit evaluation in certain special cases is considered in [6]. We define n to be the power of p dividing B

$$B = p^n B', \qquad p \nmid B'. \tag{7}$$

The evaluation in [3] relied on expressing (2) in terms of Gauss sums

$$G(\chi, p^m) := \sum_{x=1}^{p^m} \chi(x) e_{p^m}(x), \tag{8}$$

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

$$J_B(\chi_1, \ldots, \chi_s, p^m) = \chi_1 \cdots \chi_s(B') p^{-(m-n)} \overline{G(\chi_1 \cdots \chi_s, p^{m-n})} \prod_{i=1}^{s} G(\chi_i, p^m), \tag{9}$$

(see for example [3, Theorem 2.2]). In particular if $m \geqslant n + 2$ and at least one of the χ_i is primitive we see that $J_B(\chi_1, \ldots, \chi_s, p^m) = 0$ unless all the χ_i are primitive with $\chi_1\cdots\chi_s$ primitive mod p^{m-n}. In this latter case (9) and a useful evaluation of the Gauss sum led in [3] to the following explicit evaluation of (2):

$$J_B(\chi_1,\ldots,\chi_s,p^m)=p^{\frac{1}{2}(m(s-1)+n)}\frac{\chi_1(B'c_1)\cdots\chi_s(B'c_s)}{\chi_1\cdots\chi_s(v)}\delta(\chi_1,\ldots,\chi_s), \tag{10}$$

where, when p is odd,

$$\delta(\chi_1,\ldots,\chi_s)=\left(\frac{-2r}{p}\right)^{m(s-1)+n}\left(\frac{v}{p}\right)^{m-n}\left(\frac{c_1\cdots c_s}{p}\right)^{m}\varepsilon_{p^m}^{s}\varepsilon_{p^{m-n}}^{-1}, \tag{11}$$

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

$$a^{\phi(p)}=1+rp, \qquad \chi_i(a)=e_{\phi(p^m)}(c_i), \quad 1\leqslant c_i\leqslant\phi(p^m), \tag{12}$$

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

$$\varepsilon_j:=\begin{cases}1, & \text{if } \ j\equiv 1 \bmod 4,\\ i, & \text{if } \ j\equiv 3 \bmod 4,\end{cases} \qquad v:=p^{-n}(c_1+\cdots+c_s). \tag{13}$$

The sums (6) could also be expressed in terms of Gauss sums. As we shall see in Theorem 2.1 below, our general sums (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 (2) and their evaluation (10). We define the parameters t_i and t by

$$p^{t_i}\ ||\ k_i, \qquad t:=\max\{t_1,\ldots,t_s\}. \tag{14}$$

Note, it is natural to assume that $m\geqslant t+1$ (and $m\geqslant t+2$ for $p=2$, $m\geqslant 3$), since if $m\leqslant t_i$ one can replace k_i by k_i/p. We define d_i and D_i by

$$d_i:=(k_i,p-1), \qquad D_i:=\begin{cases}p^{t_i}d_i, & \text{if } p \text{ is odd},\\ 2^{t_i+1}, & \text{if } p=2,\ k_i \text{ even},\\ 1, & \text{if } p=2,\ k_i \text{ odd}.\end{cases} \tag{15}$$

Theorem 1.1. *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 be of the form* (4). *With n and t as in* (7) *and* (14) *we suppose that $m\geqslant 2t+n+2$.*

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

$$J_B(\vec{\chi},h,p^m)=D_1\cdots D_s p^{\frac{1}{2}(m(s-1)+n)}\chi_1(\alpha_1)\cdots\chi_s(\alpha_s)\delta(\chi_1',\ldots,\chi_s'), \tag{16}$$

where the c_i' define the χ_i' as in (12), *$v'=p^{-n}(c_1'+\cdots+c_s')$, $\delta(\chi_1',\ldots,\chi_s')$ is as in* (11) *with c_i' and v' replacing the c_i and v.*

Otherwise the sum is zero.

The corresponding $p=2$ result is given in Theorem 4.1.

2. Gauss sums

We first show that $J_B(\vec{\chi}, h, p^m) = 0$ unless each χ_i is a k_i-th power. We actually consider a slightly more general sum.

Lemma 2.1. *For any prime p, multiplicative characters $\chi_1, \dots, \chi_s, \chi$ mod p^m, and f, g, h in $\mathbb{Z}[x_1, \dots, x_s]$, the sum*

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

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

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

$$\begin{aligned} J &= \sum_{\substack{x_1=1 \\ h(x_1^{k_1},\dots,x_s^{k_s}) \equiv B \bmod p^m}}^{p^m} \cdots \sum_{x_s=1}^{p^m} \chi_1(x_1 z_1)\cdots\chi_s(x_s)\chi\Big(f(x_1^{k_1},\dots,x_s^{k_s})\Big)e_{p^m}\Big(g(x_1^{k_1},\dots,x_s^{k_s})\Big) \\ &= \chi_1(z_1)J. \end{aligned}$$

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

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

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

For $p = 2$ and $m \geqslant 3$ recall that $\mathbb{Z}_{2^m}^*$ needs two generators -1 and 5, where 5 has order 2^{m-2} (see for example [4]). Taking $z_1 = 5^{2^{m-2}/(k_1,2^{m-2})}$ we see that $(k_1, 2^{m-2}) \mid c_1$ and there exists a c_1' with $c_1' k_1 \equiv c_1$ 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 $i = 1, \dots, s$. ∎

From Lemma 2.1 we can thus assume that each χ_i equals a k_ith power, enabling us to express $J_B(\vec{\chi}, h, p^m)$, when h is of the form (4), in terms of (2) sums and hence, by (9), Gauss sums.

Theorem 2.1. *Let $\chi_1, \dots, \chi_s$ be mod p^m characters with $\chi_i = (\chi_i')^{k_i}$ for some characters χ_i' mod p^m character, and h be of the form (4). Then,*

$$J_B(\vec{\chi}, h, p^m) = \sum_{\substack{(\chi_i'')^{k_i} = \chi_0 \\ i=1,\dots,s}} \left(\prod_{j=1}^{s} \chi_j' \chi_j''(A_j^{-1}) \right) J_B(\chi_1'\chi_1'', \dots, \chi_s'\chi_s'', p^m), \tag{17}$$

where χ_0 is the principal character mod p^m. If $m \geqslant n+t+2$ for p odd, $m \geqslant n+t+3$ for $p=2$, and at least one of the characters is primitive mod p^m then $J_B(\vec{\chi}, h, p^m) = 0$ unless all the χ_i' are primitive mod p^m with $\chi_1' \dots \chi_s'$ induced by a primitive mod p^{m-n} character, in which case

$$J_B(\vec{\chi}, h, p^m) = \sum_{\substack{(\chi_i'')^{k_i}=\chi_0 \\ i=1,\dots,s}} \frac{\prod_{i=1}^s \chi_i'\chi_i''(A_i^{-1}B')G\left(\chi_i'\chi_i'', p^m\right)}{G\left(\chi_1'\chi_1'' \cdots \chi_s'\chi_s'', p^{m-n}\right)}. \tag{18}$$

Proof. Observe that if $p \nmid u$ then the sum

$$\sum_{\chi^{k_i}=\chi_0 \bmod p^m} \chi(u) = D_i := \begin{cases} (k_i, \phi(p^m)), & \text{if } p \text{ is odd or } p^m = 2, 4, \\ 2(k_i, 2^{m-2}), & \text{if } p=2,\ m \geqslant 3,\ k_i \text{ is even}, \\ 1, & \text{if } p=2,\ m \geqslant 3,\ k_i \text{ is odd}, \end{cases} \tag{19}$$

if u is a k_ith power (in which case $x_i^{k_i} = u$ has D_i solutions x_i) and equals zero otherwise. Hence writing $\chi_i = (\chi_i')^{k_i}$ and making the substitution $u_i \mapsto A_i^{-1}u_i$, we have

$$\begin{aligned} J_B(\vec{\chi}, h, p^m) &= \sum_{\substack{x_1=1 \\ A_1x_1^{k_1}+\cdots+A_sx_s^{k_s}\equiv B \bmod p^m}}^{p^m} \cdots \sum_{x_s=1}^{p^m} \chi_1'(x_1^{k_1}) \cdots \chi_s'(x_s^{k_s}) \\ &= \sum_{\substack{(\chi_i'')^{k_i}=\chi_0 \\ i=1,\dots,s}} \sum_{\substack{u_1=1 \\ A_1u_1+\cdots+A_su_s\equiv B \bmod p^m}}^{p^m} \cdots \sum_{u_s=1}^{p^m} \chi_1'\chi_1''(u_1) \cdots \chi_s'\chi_s''(u_s) \\ &= \sum_{\substack{(\chi_i'')^{k_i}=\chi_0 \\ i=1,\dots,s}} \overline{\chi_1'\chi_1''}(A_1) \cdots \overline{\chi_s'\chi_s''}(A_s) \\ &\quad \times \sum_{\substack{u_1=1 \\ u_1+\cdots+u_s\equiv B \bmod p^m}}^{p^m} \cdots \sum_{u_s=1}^{p^m} \chi_1'\chi_1''(u_1) \cdots \chi_s'\chi_s''(u_s), \end{aligned} \tag{20}$$

and (17) is clear. Note, if χ_i is primitive mod p^m then $\chi_i'\chi_i''$ must be primitive for all χ_i'' mod p^m with $(\chi_i'')^{k_i} = \chi_0$ (since $\chi_i = (\chi_i'\chi_i'')^{k_i}$).

Hence, by (9), if $m > n$ and at least one of the χ_i is primitive mod p^m

$$\begin{aligned} J_B(\vec{\chi}, h, p^m) = p^{-(m-n)} &\sum_{\substack{(\chi_i'')^{k_i}=\chi_0 \\ i=1,\dots,s}}^{*} \overline{G\left(\prod_{j=1}^s \chi_j'\chi_j'', p^{m-n}\right)} \\ &\times \prod_{i=1}^s \chi_i'\chi_i''(A_i^{-1}B')G\left(\chi_i'\chi_i'', p^m\right), \end{aligned} \tag{21}$$

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

$$p^{m-t_i-1} \mid c_i'' \quad \Rightarrow \quad p^{n+1} \mid c_i''. \tag{22}$$

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

$$2^{m-t-2} | c_i'' \quad \Rightarrow \quad 2^{n+1} | c_i''. \tag{23}$$

Hence $p \mid (c_i' + c_i'')$ iff $p \mid c_i'$ and $p^n \parallel \sum_{i=1}^s (c_i' + c_i'')$ iff $p^n \parallel \sum_{i=1}^s c_i'$. That is $\chi_i'\chi_i''$ is primitive mod p^m iff χ_i' is primitive mod p^m and $\prod_{i=1}^s \chi_i'\chi_i''$ is primitive mod p^{m-n} iff $\prod_{i=1}^s \chi_i'$ is primitive mod p^{m-n}. Observing that for $k \geqslant 2$ we have $G(\chi, p^k) = 0$ if χ is not primitive mod p^k we see that all the terms in (21) will be zero unless the χ_i' are all primitive mod p^m with $\prod_{i=1}^s \chi_i'$ primitive mod p^{m-n}. Observing that $|G(\chi, p^k)|^2 = p^k$ if χ is primitive mod p^k gives the form (18). ■

3. Proof of Theorem 1.1

Suppose that $m \geqslant n+t+2$ and at least one of the χ_i is primitive. From Lemma 2.1 and Theorem 2.1 we can assume that each χ_i equals $(\chi_i')^{k_i}$ for some χ_i' which is primitive mod p^m and that $\prod_{i=1}^s \chi_i'$ is primitive mod p^{m-n}, else the sum is zero. As in the proof of Theorem 2.1 we know that the $\chi_i'\chi_i''$ are all primitive mod p^m with $\prod_{i=1}^s \chi_i'\chi_i''$ primitive mod p^{m-n}. Hence using (17) and the evaluation (10) from [3] we can write

$$J_B(\vec{\chi}, h, p^m) = p^{\frac{1}{2}(m(s-1)+n)} \times \sum_{(\chi_i'')^{k_i} = \chi_0} \frac{\chi_1'\chi_1''(A_1^{-1}B'(c_1' + c_1'')) \cdots \chi_s'\chi_s''(A_s^{-1}B'(c_s' + c_s''))}{\chi_1'\chi_1'' \cdots \chi_s'\chi_s''(v)} \tilde{\delta}, \tag{24}$$

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

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

with ε_{p^m}, and r as defined in (13) and (12), with an extra factor $e_3(rv)$ needed when $p = m - n = 3$. From (22) we know that $p^{n+1} \mid c_i''$ for all i, so $c_i' + c_i'' \equiv c_i'$ mod p, $v \equiv v'$ mod p, and

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

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

$$m \geqslant n + 2t + 2. \tag{25}$$

It is perhaps worth noting that in [5] the sums (6) genuinely required a different evaluation in the range $n+t+2 \leqslant m < n+2t+2$ to that when $m \geqslant n+2t+2$. Since $p^{m-1-t_i} \mid c_i''$ we certainly have $p^{m-1-t} \mid c_i''$ and the characters χ_i'' and $\prod_{i=1}^{s} \chi_i''$ are mod p^{t+1} characters. Condition (25) ensures $p^{t+n+1} \mid c_i''$, $v \equiv v'$ mod p^{t+1} and

$$\chi_i''(c_i' + c_i'') = \chi_i''(c_i'), \qquad \chi_1'' \cdots \chi_s''(v) = \chi_1'' \cdots \chi_s''(v'). \tag{26}$$

We define the integers R_j by

$$a^{\phi(p^j)} = 1 + R_j p^j. \tag{27}$$

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 $j \geqslant i$. Defining positive integers l_i with

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

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

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

and $\chi_i'(c_i' + c_i'') = \chi_i'(c_i') e_{p^{t+1}}(c_i' l_i)$.
Since $m - t - n - 1 \geqslant t + 1$ we have $R_{m-t-1} \equiv R_{m-t-n-1}$ mod p^{t+1} and

$$\prod_{i=1}^{s} \chi_i' \chi_i''(c_i' + c_i'') = e_{p^{t+1}}(L) \prod_{i=1}^{s} \chi_i' \chi_i''(c_i'), \quad L := R_{m-t-n-1}^{-1} \sum_{i=1}^{s} c_i'' p^{-(m-t-1)}. \tag{28}$$

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

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

and

$$\begin{aligned} \chi_1'\chi_1'' \cdots \chi_s'\chi_s''(v) &= \chi_1'\chi_1'' \cdots \chi_s'\chi_s''(v') e_{\phi(p^m)}(p^n v'(v')^{-1}\phi(p^{m-t-n-1})L) \\ &= \chi_1'\chi_1'' \cdots \chi_s'\chi_s''(v') e_{p^{t+1}}(L). \end{aligned} \tag{29}$$

By substituting (28) and (29) in (24) we get

$$J_B = p^{\frac{1}{2}(m(s-1)+n)} \delta(\chi_1', \ldots, \chi_s') \sum_{\substack{(\chi_i'')^{k_i} = \chi_0 \\ i=1,\ldots,s}} \frac{\chi_1'\chi_1''(A_1^{-1}B'c_1') \cdots \chi_s'\chi_s''(A_s^{-1}B'c_s')}{\chi_1'\chi_1'' \cdots \chi_s'\chi_s''(v')} \tag{30}$$

$$= p^{\frac{1}{2}(m(s-1)+n)} \delta(\chi_1', \ldots, \chi_s') \prod_{j=1}^{s} \chi_j'(A_j^{-1}B'c_j'v'^{-1})$$

$$\times \prod_{i=1}^{s} \sum_{(\chi_i'')^{k_i} = \chi_0} \chi_i''(A_i^{-1}B'c_i'v'^{-1}).$$

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

$$J_B = D_1 \cdots D_s p^{\frac{1}{2}(m(s-1)+n)} \delta(\chi_1', \dots, \chi_s') \prod_{i=1}^{s} \chi_i'(A_i^{-1}B'c_i'v'^{-1}). \qquad \blacksquare$$

4. The case $p = 2$

As shown in [3] the sums (2) still have an evaluation (10) when $p = 2$ and $m-n \geqslant 5$, with δ now defined by

$$\delta(\chi_1, \dots, \chi_s) = \left(\frac{2}{v}\right)^{m-n} \left(\frac{2}{c_1 \cdots c_s}\right)^{m} \omega^{(2^n-1)v}, \tag{31}$$

where c_i, v, and ω are defined as

$$\chi_i(5) = e_{2^{m-2}}(c_i), \qquad 1 \leqslant c_i \leqslant 2^{m-2}, \qquad 1 \leqslant i \leqslant s, \tag{32}$$

and

$$v = 2^{-n}(c_1 + \cdots + c_s), \qquad \omega := e^{\pi i/4}. \tag{33}$$

Theorem 4.1. *Let $\chi_1, \dots, \chi_s$ be mod 2^m characters with at least one of them primitive, and h be of the form (4). Suppose that $m \geqslant 2t + n + 5$.*

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

$$J_B(\vec{\chi}, h, 2^m) = 2^{\frac{1}{2}(m(s-1)+n)} D_1 \cdots D_s\, \chi_1(\alpha_1) \cdots \chi_s(\alpha_s) \delta(\chi_1', \dots, \chi_s'), \tag{34}$$

where the c_i' are defined by $\chi_i'(5) = e_{2^{m-2}}(c_i')$, $v' = 2^{-n}\sum_{i=1}^{s} c_i'$ and $\delta(\chi_1', \dots, \chi_s')$ is as in (31) with c_i' and v' replacing the c_i and v. Otherwise the sum is zero.

Proof. Suppose first that $m \geqslant n + t + 5$ and at least one of the χ_i primitive mod 2^m. From Lemma 2.1 and Theorem 2.1 we can assume that $\chi_i = (\chi_i')^{k_i}$ with χ_i' primitive mod 2^m and $\prod_{i=1}^{s} \chi_i'$ primitive mod 2^{m-n}, else the sum is zero. As the proof in Theorem 2.1 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 (17) and the evaluation for case $p = 2$ from [3] we can write

$$J_B(\vec{\chi}, h, 2^m) = 2^{\frac{1}{2}(m(s-1)+n)} \times \sum_{(\chi_i'')^{k_i}=\chi_0} \frac{\chi_1'\chi_1''(A_1^{-1}B'(c_1'+c_1'')) \cdots \chi_s'\chi_s''(A_s^{-1}B'(c_s'+c_s''))}{\chi_1'\chi_1'' \cdots \chi_s'\chi_s''(v)} \tilde{\delta}, \tag{35}$$

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

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

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

$$c_i' + c_i'' \equiv c_i' \mod 2^{m-t-2}, \tag{36}$$

and

$$v = 2^{-n} \sum_{i=1}^{s} (c_i' + c_i'') \equiv 2^{-n} \sum_{i=1}^{s} c_i' = v' \mod 2^{m-n-t-2}. \tag{37}$$

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

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

and $\tilde{\delta} = \delta(\chi_1'\chi_1'', \ldots, \chi_s'\chi_s'') = \delta(\chi_1', \ldots, \chi_s')$. From $2^{m-t-2} \mid c_i''$ we know that the χ_i'' are all mod 2^{t+2} characters. Suppose now that $m \geqslant 2t+n+4$. Then (36) and (37) give $c_i' + c_i'' \equiv c_i' \bmod 2^{t+2}$, $v \equiv v' \bmod 2^{t+2}$, and

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

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

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

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

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

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

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

giving

$$\prod_{i=1}^{s} \chi_i'\chi_i''(c_i' + c_i'') = e_{2^{t+2}}(L) \prod_{i=1}^{s} \chi_i'\chi_i''(c_i'), \quad L := R_{m-t-n-2}^{-1} \sum_{i=1}^{s} c_i'' 2^{-(m-t-2)}. \tag{38}$$

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

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

and

$$\chi_1'\chi_1'' \cdots \chi_s'\chi_s''(v) = \chi_1'\chi_1'' \cdots \chi_s'\chi_s''(v') e_{2^{t+2}}(L). \tag{39}$$

By substituting (38) and (39) in (35) we get (30) and the rest of the proof follows unchanged from p odd. ∎

5. Imprimitive characters or non-prime power moduli

We assumed in Theorem 1.1 that at least one of the characters is primitive mod p^m. This is a fairly natural assumption, for example if $p \nmid k_i$ for at least one i and none of the χ_i are primitive mod p^m then we can reduce to a mod p^{m-1} sum.

Lemma 5.1. *Let p be an odd prime and h be of the form (4). If $\chi_1, \ldots, \chi_s$ are imprimitive characters mod p^m with $p \nmid k_i$ for some i and $m \geqslant 2$, then*

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

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

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

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

$$\sum_{i=1}^s A_i(u_i+v_i p^{m-1})^{k_i} \equiv \sum_{i=1}^s A_i u_i^{k_i} + p^{m-1} \left(\sum_{i=1}^s A_i k_i u_i^{k_i-1} v_i \right) \equiv B \mod p^m, \quad (40)$$

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

$$\sum_{i=1}^s A_i u_i^{k_i} \equiv B \mod p^{m-1}, \quad (41)$$

and for any $u_1, \ldots, u_s$ satisfying (41), to satisfy (40) the v_i must satisfy

$$\sum_{i=1}^s A_i k_i u_i^{k_i-1} v_i \equiv p^{-(m-1)} \left(B - \sum_{i=1}^s A_i u_i^{k_i} \right) \mod p. \quad (42)$$

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 (42)

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

and

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

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

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

When q is composite the following lemma can be used to reduce sums of the form (3) to the case of prime power modulus.

Lemma 5.2. *Suppose that $\chi_1, \ldots, \chi_s$ are mod uv characters with $(u, v) = 1$. Writing $\chi_i = \chi_i' \chi_i''$ for mod u and mod v characters χ_i' and χ_i'' respectively, then*

$$J_B(\vec{\chi}, h, uv) = J_B(\vec{\chi'}, h, u) J_B(\vec{\chi''}, h, v).$$

Proof. Suppose that χ_i are mod uv characters with $(u, v) = 1$, and $\chi_i = \chi_i'\chi_i''$, where χ_i' is a mod u and χ_i'' a mod v character. Writing $x_i = e_i v v^{-1} + f_i u u^{-1}$, where $uu^{-1} + vv^{-1} = 1$ and $e_i = 1, \ldots, u$, $f_i = 1, \ldots, v$, gives

$$\begin{aligned} J_B(\vec{\chi}, h, uv) &= \sum_{\substack{e_1=1 \\ h(e_1vv^{-1}+f_1uu^{-1},\ldots,e_svv^{-1}+f_suu^{-1})\equiv B \bmod u \\ h(e_1vv^{-1}+f_1uu^{-1},\ldots,e_svv^{-1}+f_suu^{-1})\equiv B \bmod v}}^{u} \sum_{f_1=1}^{v} \cdots \sum_{e_s=1}^{u} \sum_{f_s=1}^{v} \chi_1(e_1 vv^{-1} + f_1 uu^{-1}) \cdots \chi_s(e_s vv^{-1} + f_s uu^{-1}) \\ &= \sum_{\substack{e_1=1 \\ h(e_1,\ldots,e_s)\equiv B \bmod u}}^{u} \cdots \sum_{e_s=1}^{u} \chi_1'(e_1)\cdots\chi_s'(e_s) \sum_{\substack{f_1=1 \\ h(f_1,\ldots,f_s)\equiv B \bmod v}}^{v} \cdots \sum_{f_s=1}^{v} \chi_1''(f_1)\cdots\chi_s''(f_s) \\ &= J_B(\vec{\chi'}, h, u) J_B(\vec{\chi''}, h, v). \end{aligned}$$

■

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 and Z. Zheng, *Pure and mixed exponential sums*, Acta Arith. **91** (1999), no. 3, 249–278.

[3] M. Long, V. Pigno, and C. Pinner, *Evaluating Prime Power Gauss and Jacobi Sums*, arXiv:1410.6179 [math.NT].

[4] I. Niven, H.S. Zuckerman, and H. L. Montgomery, *An Introduction to The Theory of Numbers*, 5th edition, John Wiley & Sons, Inc. 1991.

[5] V. Pigno and C. Pinner, *Binomial Character Sums Modulo Prime Powers*, J. Théor. Nombres Bordeaux **28** (2016), no. 1, 39–53.

[6] W. Zhang and T. Wang, *A note on the Dirichlet characters of polynomials*, Math. Slovaca **64** (2014), no. 2, 301–310.
[7] W. Zhang and W. Yao, *A note on the Dirichlet characters of polynomials*, Acta Arith. **115** (2004), no. 3, 225–229.
[8] W. Zhang and Z. Xu, *On the Dirichlet characters of polynomials in several variables*, Acta Arith. **121** (2006), no. 2, 117–124.

Addresses: Badria Alsulmi: Department of Mathematics, Umm al-Quara University, Mecca 24382, Saudi Arabia;
Vincent Pigno: Department of Mathematics & Statistics, California State University, Sacramento, Sacramento, CA 95819, USA;
Christopher Pinner: Department of Mathematics, Kansas State University, Manhattan, KS 66506, USA.

E-mail: bmsulmi@uqu.edu.sa, vincent.pigno@csus.edu, pinner@math.ksu.edu

Received: 7 March 2016; **revised:** 3 October 2016