JACOBI-TYPE SUMS WITH AN EXPPLICIT EVALUATION
MODULO PRIME POWERS

BADRIA ALSULMI, VINCENT PIGNO, AND CHRISTOPHER PINNER

Abstract. We show that for Dirichlet character \( \chi_1, \ldots, \chi_s \mod p^m \) the sum
\[
\sum_{x_1=1}^{p^m} \cdots \sum_{x_s=1}^{p^m} \chi_1(x_1) \cdots \chi_s(x_s)
\]
has a simple evaluation when \( m \) is sufficiently large.

1. Introduction

For two Dirichlet characters \( \chi_1, \chi_2 \mod q \) the classical Jacobi sum is
\[
J(\chi_1, \chi_2, q) := \sum_{x=1}^{q} \chi_1(x)\chi_2(1-x).
\]
More generally, for \( s \) characters \( \chi_1, \ldots, \chi_s \mod q \) and an integer \( B \), one can define a generalized Jacobi sum
\[
J_B(\chi_1, \ldots, \chi_s, q) := \sum_{x_1=1}^{q} \cdots \sum_{x_s=1}^{q} \chi_1(x_1) \cdots \chi_s(x_s) \equiv B \mod q.
\]
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) had an explicit evaluation when \( q \) is a perfect square and Zhang & Xu 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 \( \chi_i \mod q \), then for an \( h \in \mathbb{Z}[x_1, \ldots, x_s] \) and \( B \in \mathbb{Z} \) we can define
\[
J_B(\vec{\chi}, h, q) := \sum_{x_1=1}^{q} \cdots \sum_{x_s=1}^{q} \chi_1(x_1) \cdots \chi_s(x_s) \equiv B \mod q.
\]

Date: October 27, 2014.
2010 Mathematics Subject Classification. Primary:11L10, 11L40; Secondary:11L03,11L05.
Key words and phrases. Character Sums, Gauss sums, Jacobi Sums.
The second author acknowledges support of California State University, Sacramento’s Provost’s Research Incentive Fund.
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
\[
h(x_1, \ldots, x_s) = A_1x_1^{k_1} + \cdots + A_s x_s^{k_s}, \quad p \nmid A_1 \cdots A_s,
\]
where the \( k_i \) are non-zero integers, and
\[
J_B(\chi, h, p^m) = \sum_{x_i=1}^{p^m} \cdots \sum_{x_s=1}^{p^m} \chi_1(x_1) \cdots \chi_s(x_s).
\]

As well as (2) this generalization includes the binomial character sums
\[
\sum_{x=1}^{p^m} \chi_1(x)\chi_2(Ax^k + B)
\]
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 \( B = p^s B', \quad p \nmid B' \).

The evaluation in [3] relied on expressing (2) in terms of Gauss sums
\[
G(\chi, p^m) := \sum_{x=1}^{p^m} \chi(x)e_{p^m}(x),
\]
where \( e_k(x) = e^{2\pi i x/k} \). For example, if at least one of the \( \chi_i \) is primitive mod \( p^m \) and \( m > n \) then \( J_B(\chi_1, \ldots, \chi_s, p^m) = 0 \) unless \( \chi_1 \cdots \chi_s \) is a mod \( p^{m-n} \) character, in which case
\[
J_B(\chi_1, \ldots, \chi_s, p^m) = \chi_1 \cdots \chi_s(B')p^{-(m-n)}G(\chi_1, \ldots, \chi_s, p^{m-n}) \prod_{i=1}^{s} G(\chi_i, p^m)
\]
(see for example [3, Theorem 2.2]). In particular if \( m \geq n + 2 \) and at least one of the \( \chi_i \) is primitive we see that \( J_B(\chi_1, \ldots, \chi_s, p^m) = 0 \) unless all the \( \chi_i \) are primitive with \( \chi_1 \cdots \chi_s \) primitive mod \( p^{m-n} \). In this latter case (9) and a useful evaluation of the Gauss sum led in [3] to the following explicit evaluation of (2):
\[
J_B(\chi_1, \ldots, \chi_s, p^m) = p^{\frac{1}{2}(m(s-1)+n)} \frac{\chi_1(B'c_1) \cdots \chi_s(B'c_s)}{\chi_1 \cdots \chi_s(c)} \delta(\chi_1, \ldots, \chi_s),
\]
with, when \( p \) is odd,
\[
\delta(\chi_1, \ldots, \chi_s) = \left( -\frac{2r}{p} \right)^{m(s-1)+n} \left( \frac{v}{p} \right)^{m-n} \left( \frac{c_1 \cdots c_s}{p} \right)^m \varepsilon_{p^m}^{-1} \varepsilon_{p^m-n}^{-1}
\]
where, for a choice of primitive root \( a \mod p^m \), the integers \( r \) and \( c_i \) are defined by
\[
a^{\phi(p^m)} = 1 + rp, \quad \chi_i(a) = e_{p^m}(c_i), \quad 1 \leq c_i \leq \phi(p^m),
\]
as usual \( \left( \frac{a}{p} \right) \) denotes the Jacobi symbol, and
\[
\varepsilon_j := \begin{cases} 1, & \text{if } j \equiv 1 \mod 4, \\ i, & \text{if } j \equiv 3 \mod 4 \end{cases}, \quad v := p^{-n}(c_1 + \cdots + c_k).
\]
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

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

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

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

**Theorem 1.1.** Let \( p \) be an odd prime, \( \chi_1, \ldots, \chi_s \) be mod \( p^n \) 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 \( m \geq 2t + n + 2 \).

If the \( \chi_i = (\chi_i')^{k_i} \) for some primitive characters \( \chi_i' \) mod \( p^n \) such that \( \chi_1' \cdots \chi_s' \) is induced by a primitive mod \( p^{m-n} \) character, and the \( A^{-1}Bc_i^{v-1} \equiv \alpha_i^{k_i} \mod p^n \) for some \( \alpha_i \), then

\[
J_B(\vec{x}, h, p^n) = D_1 \cdots D_s p^{\frac{1}{2}(m-1)+n} \chi_1(\alpha_1) \cdots \chi_s(\alpha_s) \delta(\chi_1', \ldots, \chi_s'),
\]

where the \( c_i' \) define the \( \chi_i' \) as in (12), \( v' = p^{-n}(c_1' + \cdots + c_s') \), and \( \delta(\chi_1', \ldots, \chi_s') \) 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 \( J_B(\vec{x}, h, p^n) = 0 \) unless each \( \chi_i \) is a \( k_i \)-th power. We actually consider a slightly more general sum.

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

\[
J = \sum_{x_1}^{p^m} \cdots \sum_{x_s}^{p^m} \chi_1(x_1) \cdots \chi_s(x_s) \chi(f(x_1^{k_1}, \ldots, x_s^{k_s})) e_{p^n}(g(x_1^{k_1}, \ldots, x_s^{k_s})),
\]

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

**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

\[
J = \sum_{x_1}^{p^m} \cdots \sum_{x_s}^{p^m} \chi_1(x_1 z_1) \cdots \chi_s(x_s) \chi(f(x_1^{k_1}, \ldots, x_s^{k_s})) e_{p^n}(g(x_1^{k_1}, \ldots, x_s^{k_s}))
\]

\[
= \chi_1(z_1) J.
\]

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

\[
c_1 \equiv c_1' k_1 \mod \phi(p^n),
\]

where \( c_1' \) is a primitive root mod \( p^n \).
and \( \chi_1 = (\chi'_1)^k_i \) where \( \chi'_1 \) is the mod \( p^m \) character with \( \chi'_1(a) = c_{\phi(p^m)}(e_i') \).

For \( p = 2 \) and \( m \geq 3 \) recall that \( \mathbb{Z}_{2^m}^\times \) 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 \( (k_1, 2^{m-2}) \mid e_1 \) and there exists a \( e'_1 \) with \( e'_1 k_1 \equiv e_1 \mod 2^{m-2} \). Setting

\[
\chi'_1(-1) = \chi_1(-1), \quad \chi'_1(5) = e_{2^{m-2}}(e'_1),
\]

we have \( \chi_1(5) = (\chi'_1(5))^{k_i} \). If \( k_1 \) is odd then \( \chi_1(-1) = (\chi'_1(-1))^{k_i} \). If \( k_1 \) is even then \( z_1 = -1 \) gives \( \chi_1(-1) = 1 = (\chi'_1(-1))^{k_i} \). Hence \( \chi_1 = (\chi'_1)^{k_i} \).

The same technique gives \( \chi_i = (\chi'_i)^{k_i} \) for all \( i = 1, \ldots, s \).

\[ \square \]

From Lemma 2.1 we can thus assume that the \( \chi_i \) are \( k_i \)th powers, enabling us to express \( J_B(\tilde{\chi}, h, \tilde{A}, p^m) \) in terms of (2) sums and hence, by (10), Gauss sums.

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

\[
J_B(\tilde{\chi}, h, p^m) = \sum_{(\chi'_i)^{k_i} = \chi_0} \prod_{j=1}^{s} \chi'_j(A_j^{-1}) J_B(\chi'_1, \ldots, \chi'_s, p^m),
\]

where \( \chi_0 \) is the principal character mod \( p^m \). If \( m \geq n + t + 2 \) for \( p \) odd, \( m \geq n + t + 3 \) for \( p = 2 \), and at least one of the characters is primitive mod \( p^m \) then \( J_B(\tilde{\chi}, h, p^m) = 0 \) unless all the \( \chi'_i \) are primitive mod \( p^m \) with \( \chi'_1 \cdots \chi'_s \) induced by a primitive mod \( p^{m-n} \) character, in which case

\[
J_B(\tilde{\chi}, h, p^m) = \sum_{(\chi'_i)^{k_i} = \chi_0} \prod_{j=1}^{s} \chi'_j(A_j^{-1} B') G(\chi'_1, \ldots, \chi'_s, p^{m-n}).
\]

**Proof.** Writing \( \chi_i = (\chi'_i)^{k_i} \), observing that if \( p \mid u \) then the sum

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

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

\[
J_B(\tilde{\chi}, h, p^m) = \sum_{A_1 x_1^{k_1} + \cdots + A_s x_s^{k_s} \equiv B \mod p^m} \chi'_1(x_1^{k_1}) \cdots \chi'_s(x_s^{k_s})
\]

\[
= \sum_{(\chi'_i)^{k_i} = \chi_0} \prod_{i=1}^{\frac{s}{k_i}} \sum_{u_i=1}^{p^m} \chi'_1(u_1) \cdots \chi'_s(u_s)
\]

\[
= \sum_{(\chi'_i)^{k_i} = \chi_0} \frac{\chi'_1(A_1) \cdots \chi'_s(A_s)}{A_1 u_1 + \cdots + A_s u_s \equiv B \mod p^m}
\]

\[
= \sum_{(\chi'_i)^{k_i} = \chi_0} \sum_{u_1=1}^{p^m} \cdots \sum_{u_s=1}^{p^m} \chi'_1(u_1) \cdots \chi'_s(u_s),
\]
and (17) is clear. Note, if \( \chi_i \) is primitive mod \( p^m \) then \( \chi_i' \chi_i'' \) must be primitive for all \( \chi_i' \mod p^m \) with \( (\chi_i')^k = 0 \) (since \( \chi_i = (\chi_i')^{k_i} \)).

Hence, by (10), if \( m > n \) and at least one of the \( \chi_i \) is primitive mod \( p^m \)

\[
J_B(\chi, h, p^m) = p^{-(m-n)} \sum_{(\chi''_i)^{k_i}=0}^{*} G \left( \prod_{i=1}^{s} \chi''_i(A_i^{-1}B') \right) \prod_{i=1}^{s} \chi''_i(A_i^{-1}B') G \left( \chi''_i, p^m \right),
\]

where the * indicates the sum is restricted to the \( \chi''_i \mod p^m \) such that \( \prod_{i=1}^{s} \chi''_i \) is a \( m \) primitive character. Suppose further that \( m \geq n + t + 2 \) and \( p \) is odd. Since \( (\chi''_i)^{k_i} = 0 \), that is \( e_{\phi(p^m)}(c'_i|k_i) = 1 \), then

\[
p^{m-t-1} \mid c''_i = p^{n+1} \mid c''_i.
\]

Likewise for \( p = 2 \), if \( (\chi''_i)^{k_i} = 0 \) and \( m \geq n + t + 3 \), we have

\[
2^{m-t-2} \mid c''_i = 2^{n+2} \mid c''_i.
\]

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

\[\square\]

3. PROOF OF THEOREM 1.1

Suppose that \( m \geq n + t + 2 \) and at least one of the \( \chi_i \) is primitive. From Lemma 2.1 and Theorem 2.1 we can assume that the \( \chi_i = (\chi_i')^{k_i} \), with the \( \chi_i' \) primitive mod \( p^m \) and \( \prod_{i=1}^{s} \chi_i' \) primitive mod \( p^{m-n} \), else the sum is zero. As in the proof of Theorem 2.1 we know that all 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

\[
J_B(\chi, h, p^m) = p^{\frac{m}{2}(m-1)+n} \sum_{(\chi''_i)^{k_i}=0}^{*} \frac{\chi_i' \chi_i''(A_i^{-1}B'(c'_i + c''_i)) \cdots \chi_i''(A_i^{-1}B'(c'_i + c''_i))}{\chi_i''(v)} \delta
\]

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

\[
\delta = \delta(\chi_i' \chi''_i, \ldots, \chi_i' \chi''_i) = \left( \frac{-2r}{p} \right)^{m(s-1)+n} \left( \frac{v}{p} \right)^{m-n} \left( \frac{\prod_{i=1}^{s} (c'_i + c''_i)}{p} \right)^m \epsilon_{p^m} \epsilon_{p^{m-n}}
\]

with \( \epsilon_{p^m} \), and \( r \) as defined in (13) and (12). 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

\[
\delta = \delta(\chi_i' \chi''_i, \ldots, \chi_i' \chi''_i) = \delta(\chi_i', \ldots, \chi_i'),
\]

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

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

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

\[ \chi_i^{\prime}(c_i^{\prime} + c_i^{\prime}) = \chi_i^{\prime}(c_i^{\prime}), \quad \chi_1^{\prime} \cdots \chi_s^{\prime}(v) = \chi_1^{\prime} \cdots \chi_s^{\prime}(v'). \]

We define the integers \( R_j \) by

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

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 \( R_j \equiv R_0 \mod p^i \) for all \( j \geq i \). Defining positive integers \( l_i \) with

\[ l_i = (c_i^{\prime})^{-1}(c_i^{\prime} p^{-m-1-t_i}) R_{m-t-1}^{-1} \mod p^m \]

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

\[ c_i^{\prime} + c_i^{\prime} \equiv c_i^{\prime} (1 + l_i R_{m-t-1} p^{m-1-t_i}) \mod p^m \]

\[ \equiv c_i^{\prime} (1 + R_{m-t-1} p^{m-1-t_i}) \mod p^m \]

\[ \equiv c_i^{\prime} a^{\phi(p^{m-1-t_i})} \mod p^m, \]

and \( \chi_i^{\prime}(c_i^{\prime} + c_i^{\prime}) = \chi_i^{\prime}(c_i^{\prime}) a^{\phi(p^{m-1-t_i})} \).

Since \( m-t-n-1 \geq t+1 \) we have \( R_{m-t-1} \equiv R_{m-t-n-1} \mod p^{t+1} \) and

\[ \prod_{i=1}^{s} \chi_i^{\prime}(c_i^{\prime} + c_i^{\prime}) = e_{p^{t+1}}(L) \prod_{i=1}^{s} \chi_i^{\prime}(c_i^{\prime}), \quad L := R_{m-t-n-1}^{-1} \sum_{i=1}^{s} c_i^{\prime} p^{-(m-1-t_i)}. \]

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

\[ v = v' + p^{-n}(c_1^{\prime} + \cdots + c_s^{\prime}) \]

\[ \equiv v' \left( 1 + (v')^{-1} L R_{m-n-t-1} p^{m-n-1-t_i} \right) \mod p^m \]

\[ \equiv v' a^{(v')^{-1} \phi(p^{m-n-1-t_i})} L \mod p^{m-n}, \]

and

\[ \chi_1^{\prime} \chi_1^{\prime} \cdots \chi_s^{\prime} \chi_s^{\prime}(v) = \chi_1^{\prime} \chi_1^{\prime} \cdots \chi_s^{\prime} \chi_s^{\prime}(v') a^{\phi(p^{m-n-t_i})} (p^{n-1} v' \phi(p^{m-n-t_i}) L) \]

\[ = \chi_1^{\prime} \chi_1^{\prime} \cdots \chi_s^{\prime} \chi_s^{\prime}(v') e_{p^{t+1}}(L). \]

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

\[ J_B = p^{\frac{1}{2}(m-s-1)n} \delta(\chi_1^{\prime}, \ldots, \chi_s^{\prime}) \sum_{\substack{|x_i^{\prime}|_{k_i} = x_0 \\ i = 1, \ldots, s}} \chi_1^{\prime} \chi_1^{\prime} (A_1^{\prime-1} B \prime c_1^{\prime}) \cdots \chi_s^{\prime} \chi_s^{\prime} (A_s^{\prime-1} B \prime c_s^{\prime}) \chi_1^{\prime} \chi_1^{\prime} \cdots \chi_s^{\prime} \chi_s^{\prime}(v') \]

\[ = p^{\frac{1}{2}(m-s-1)n} \delta(\chi_1^{\prime}, \ldots, \chi_s^{\prime}) \prod_{j=1}^{s} \chi_j^{\prime} (A_j^{\prime-1} B \prime c_j^{\prime} v' \prime^{-1}) \prod_{i=1}^{s} \sum_{(x_i^{\prime})_{k_i} = x_0} \chi_i^{\prime} (A_i^{\prime-1} B \prime c_i^{\prime} v' \prime^{-1}). \]

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

\[ J_B = D_1 \cdots D_s p^{\frac{1}{2}(m-s-1)n} \delta(\chi_1^{\prime}, \ldots, \chi_s^{\prime}) \prod_{i=1}^{s} \chi_i^{\prime} (A_i^{\prime-1} B \prime c_i^{\prime} v' \prime^{-1}). \]
4. The Case $p = 2$

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

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

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

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

and

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

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

If the $\chi_i = (\chi'_i)^{k_i}$, for some primitive characters $\chi'_1 \ldots \chi'_s$ mod $2^m$ such that $\chi'_1 \ldots \chi'_s$ is induced by a primitive mod $2^{m-n}$ character, and the $A_i^{-1}B_i'v_i^{-1} \equiv c_i^{k_i}$ mod $2^m$ for some $\alpha_i$, then

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

where the $c'_i$ are defined by $\chi'_i(5) = e_{2m-2}(c'_i)$, $v' = 2^{-n}\sum_{i=1}^s c'_i$ and $\delta(\chi'_1, \ldots, \chi'_s)$ is as in (31) with $c'_i$ and $v'$ replacing the $c_i$ and $v$. Otherwise the sum is zero.

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

$$J_B(\chi, h, 2^m) = 2^{\frac{1}{2}(m(s-1)+n)} \sum_{(\chi''_i)^{k_i}=\chi_0} \frac{\chi''_1 \chi''_2 \cdots \chi''_s (A^{-1}_1 B'_1 (c''_1 + c''_2) \cdots \chi''_s (A^{-1}_s B'_s (c''_s + c''_s)))}{\chi''_1 \chi''_2 \cdots \chi''_s (v')},$$

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

$$\tilde{\delta} = \delta(\chi''_1, \ldots, \chi''_s) = \left(\frac{2}{v}\right)^{m-n} \left(\frac{2}{\prod_{i=1}^s (c''_i + c''_i)}\right)^m \omega(2^{n-1})^v.$$

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

$$c''_i \equiv c''_i \mod 2^{m-t-2},$$

and

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

So for $m \geq n + t + 5$ we have $c''_i + c''_i \equiv c''_i \mod 8$, $v \equiv v' \mod 8$, giving

$$\left(\frac{2}{c''_i + c''_i}\right) = \left(\frac{2}{c''_i}\right), \quad \left(\frac{v}{v'}\right) = \left(\frac{v'}{p}\right), \quad \omega(2^{n-1}) = \omega(2^{n-1})^{v'}. $$
Proof. Suppose that \( \delta = \delta(\chi_1, \chi_2', \ldots, \chi_n') = \delta(\chi_1', \ldots, \chi_n'). \) From \( 2^{m-t-2} | c_i' \) we know that the \( \chi_i'' \) are all mod \( 2^{t+2} \) characters. Suppose now that \( m \geq 2t + n + 4 \). Then (36) and (37) give \( c_i' + c_i'' \equiv c_i' \) mod \( 2^{t+2} \), \( v \equiv v' \) mod \( 2^{t+2} \), and 
\[
\chi_i''(c_i' + c_i'') = \chi_i''(c_i'), \hspace{1cm} \chi_1'' \cdots \chi_n''(v) = \chi_1'' \cdots \chi_n''(v').
\]
For \( p = 2 \) we define the integers \( R_j, j \geq 2 \) by
\[
5^{2^{t-2} - 1} = 1 + Rj2^i.
\]
From \( R_{i+1} \equiv R_i + 2^{i-1}R_i^2 \) we have the relationship \( R_j \equiv R_i \) mod \( 2^{i-1} \) for all \( j \geq i \geq 2 \). Define a positive integer \( i := (c_i')^{-1}c_i''2^{-(m-t-2)}R_{m-t-2}^{-1} \) mod \( 2^m \). Since \( 2(m-t-2) \geq m \) we have
\[
\begin{align*}
&c_i' + c_i'' \equiv c_i' (1 + b_iR_{m-t-2}2^{m-t-2}) \mod 2^m \\
&\equiv c_i' (1 + R_{m-t-2}2^{m-t-2})^i \mod 2^m \\
&\equiv c_i'5^{i-2m-1} \mod 2^m,
\end{align*}
\]
and \( \chi_i'(c_i' + c_i'') = \chi_i'(c_i'c_{2i+1}(c_i'_{1i}) \). If \( m \geq 2t + n + 5 \), then
\[
R_{m-t-2} \equiv R_{m-t-n-2} \mod 2^{m-t-n-3} \equiv R_{m-t-n-2} \mod 2^{t+2}
\]
giving
\[
(38) \sum_{1}^{n} \chi_i'(c_i' + c_i'') = e_{2^{t+2}}(L) \prod_{1}^{n} \chi_i'(c_i'_{1i}), \hspace{1cm} L := R_{m-t-n-2}^{-1} \sum_{1}^{n} c_i''2^{-(m-t-2)}.
\]
Similarily, since \( 2(m-n-t-2) \geq m-n \),
\[
\begin{align*}
v &= v' + 2^{-n}(c_i'' + \cdots + c_n'') \\
&\equiv v' (1 + (v')^{-1}LR_{m-n-t-2}2^{m-n-t-2}) \\
&\equiv v'5^{(v')^{-1}2^{m-n-1-4}L} \mod 2^{m-n},
\end{align*}
\]
and
\[
(39) \chi_1'' \chi_2'' \cdots \chi_n''(v) = \chi_1'' \chi_2'' \cdots \chi_n''(v)e_{2^{t+2}}(L).
\]
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 \( \chi_i \) 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 \( m \geq 2 \), then
\[
J_B(\chi, h, p^m) = p^{-1}J_B(\chi, h, p^{m-1}).
\]

**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
\[
J_B(\chi, h, p^m) = \sum_{\substack{u_1, \ldots, u_s=1 \atop v_1, \ldots, v_s=1}}^{p^{m-1}} \chi_1(u_1) \cdots \chi_s(u_s)
\]
where the $\chi^i(u_i)$ allow us to restrict to $(u_i,p) = 1$. Expanding we see that
\begin{equation}
\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,
\end{equation}
as long as $m \geq 2$. Thus the $u_i$ must satisfy
\begin{equation}
\sum_{i=1}^{s} A_i u_i^{k_i} \equiv B \mod p^{m-1}
\end{equation}
and for any $u_1, \ldots, u_s$ satisfying (41), to satisfy (40) the $v_i$ must satisfy
\begin{equation}
\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.
\end{equation}
If $p$ does not divide one of the exponents, $p \nmid k_i$ 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)
\[ v_1 \equiv \left( B - \sum_{i=1}^{s} A_i u_i^{k_i} \right) \sum_{i=2}^{s} A_i k_i u_i^{k_i-1} v_i \equiv \left( A_1 k_1 u_1^{k_1-1} \right)^{-1} \mod p, \]
and
\[ J_B(\vec{\chi}, h, p^m) = p^{s-1} \sum_{u_1, \ldots, u_s = 1}^{p^{m-1}} \chi_1(u_1) \cdots \chi_s(u_s) \equiv p^{s-1} J_B(\vec{\chi}, h, p^{m-1}) \mod p^{m-1} \]
\[ \sum_{i=1}^{s} A_i u_i^{k_i} \equiv B \mod p^{m-1} \]
\[ \square \]

If the $\chi_i$ are all imprimitive mod $p^m$ and $p \mid k_i$ for all $i$ then we still reduce to a mod $p^{m-1}$ sum, but as with a Heilbronn sum it seems unlikely that there is a nice evaluation:
\[ J_B(\vec{\chi}, h, p^m) = p^s \sum_{x_1=1}^{p^{m-1}} \cdots \sum_{x_s=1}^{p^{m-1}} \chi_1(x_1) \cdots \chi_s(x_s), \]
\[ A_1 x_1^{k_1} + \cdots + A_s x_s^{k_s} \equiv B \mod p^m \]

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 $\chi'_i$ and $\chi''_i$ respectively, then
\[ J_B(\vec{\chi}, h, uv) = J_B(\vec{\chi'}, h, u) J_B(\vec{\chi''}, h, v). \]

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

\[
J_B(\vec{\chi}, h, uv) = \sum_{e_1 = 1}^{u} \sum_{f_1 = 1}^{v} \cdots \sum_{e_s = 1}^{u} \sum_{f_s = 1}^{v} \chi_1(e_1uv^{-1} + f_1uu^{-1}) \cdots \chi_s(e_suv^{-1} + f_suu^{-1}),
\]

\[
h(e_1uv^{-1} + f_1uu^{-1}, \ldots, e_suv^{-1} + f_suu^{-1}) \equiv B \mod u
\]

\[
h(e_1uv^{-1} + f_1uu^{-1}, \ldots, e_suv^{-1} + f_suu^{-1}) \equiv B \mod v
\]

\[
= \sum_{e_1 = 1}^{u} \cdots \sum_{e_s = 1}^{u} \chi_1'(e_1) \cdots \chi'_s(e_s) \sum_{f_1 = 1}^{v} \cdots \sum_{f_s = 1}^{v} \chi''_1(f_1) \cdots \chi''_s(f_s).
\]

\[
h(e_1, \ldots, e_s) \equiv B \mod u
\]

\[
h(f_1, \ldots, f_s) \equiv B \mod v
\]

\[
= J_B(\vec{\chi}', h, u)J_B(\vec{\chi}'', h, v).
\]

□

References


Department of Mathematics, Kansas State University, Manhattan, KS 66506
E-mail address: badria@math.ksu.edu

Department of Mathematics & Statistics, University of California, Sacramento, Sacramento, CA 95819
E-mail address: vincent.pigno@csus.edu

Department of Mathematics, Kansas State University, Manhattan, KS 66506
E-mail address: pinner@math.ksu.edu