ACTA ARITHMETICA
126.3 (2007)

# Exponential sums of the form $\sum \chi(x)^{ax}\zeta_m^{bx}$

by

S. Gurak (San Diego, CA)

*This paper is dedicated to Basil Gordon on the occasion of his 75th birthday*

**1. Introduction.** For any integer $m > 1$ fix $\zeta_m = \exp(2\pi i/m)$ and let $\mathbb{Z}_m^*$ denote the group of reduced residues modulo $m$. Let $a$ be any integer satisfying $a \equiv 0 \pmod{p-1}$ for each prime $p \mid m$, and consider an exponential sum of the form

$$S(a,b,\chi,m) = \sum_{x\in\mathbb{Z}_m^*} \chi(x)^{ax}\zeta_m^{bx}, \tag{1}$$

where $\chi$ is any numerical character defined modulo $m$ and $b$ any integer. The sum (1) is readily expressed as a product of such sums defined for the prime powers dividing $m$. Indeed, if $m = p_1^{\alpha_1}\cdots p_r^{\alpha_r}$ is a product of distinct prime powers, decompose $\chi = \prod_{i=1}^r \chi_i$ as a product of its $p$-components. Specifically, for any $x$ prime to $p_i$, set $\chi_i(x) = \chi(x')$ with $x' \equiv x \pmod{p_i^{\alpha_i}}$ and $x' \equiv 1 \pmod{m_i}$ where $m_i = mp_i^{-\alpha_i}$ $(1 \le i \le r)$. Then

Proposition 1. *We have*

$$S(a,b,\chi,m) = \prod_{i=1}^r S(a, bc_i, \chi_i, p_i^{\alpha_i})$$

*where the $c_i$ are integers satisfying $c_i m_i \equiv 1 \pmod{p_i^{\alpha_i}}$ for $1 \le i \le r$.*

*Proof.* The choice of the $c_i$ gives $c_1m_1 + \cdots + c_rm_r \equiv 1 \pmod m$. Thus a typical term of $\prod_{i=1}^r S(a,bc_i,\chi_i,p_i^{\alpha_i})$ has the form

$$\chi_1(x_1)^{ax_1}\cdots\chi_r(x_r)^{ax_r}\zeta_{p_1^{\alpha_1}}^{bc_1x_1}\cdots\zeta_{p_r^{\alpha_r}}^{bc_rx_r} = \chi_1(x)^{ax}\cdots\chi_r(x)^{ax}\zeta_m^{bx} = \chi(x)^{ax}\zeta_m^{bx}$$

with $x = c_1m_1x_1 + \cdots + c_rm_rx_r$, one for each choice of $x_i \in \mathbb{Z}_{p_i^{\alpha_i}}^*$ $(1 \le i \le r)$, since $\chi_i^{am_j} = 1$ for $1 \le i \ne j \le r$. But as the $x_i$ independently run

2000 *Mathematics Subject Classification*: Primary 11L03, 11T23.

through $\mathbb{Z}^*_{p_i^{\alpha_i}}$ $(1 \le i \le r)$, $x$ runs through $\mathbb{Z}^*_m$. Thus $\prod_{i=1}^r S(a, bc_i, \chi_i, p_i^{\alpha_i}) = S(a, b, \chi, m)$.

The above result reduces the determination of any sum (1) to the prime power case. My principal aim here is to explicitly evaluate the sums

$$S(a, b, \chi, q) = \sum_{x \in \mathbb{Z}^*_q} \chi(x)^{ax} \zeta_q^{bx} \tag{2}$$

for prime powers $q = p^\alpha$ with $a \equiv 0 \pmod{p-1}$. While there is an extensive literature [4] concerning exponential sums of the form $\sum \chi(g(x))\zeta_q^{f(x)}$ for suitable types of functions $f(x)$ and $g(x)$, the choice $f(x) = bx$ and $g(x) = \exp(x \log x^a)$ made here seems to have been overlooked. Indeed, I have found an elegant explicit evaluation of the sums (2).

To proceed I first make some elementary observations. When $q = p$, one trivially obtains

$$S(a, b, \chi, p) = \begin{cases} p-1 & \text{if } b \equiv 0 \pmod{p}, \\ -1 & \text{if } b \not\equiv 0 \pmod{p}, \end{cases}$$

and for $b \equiv 0 \pmod{p}$ one finds the following reduction formula:

Proposition 2. *For $b \equiv 0 \pmod{p}$ in (2) with $\alpha > 1$,*

$$S(a, b, \chi, p^\alpha) = \begin{cases} pS(a/p, b/p, \chi^p, p^{\alpha-1}) & \text{if } a \equiv 0 \pmod{p}, \\ pS(a, b/p, \chi, p^{\alpha-1}) & \text{if } \chi \text{ is imprimitive modulo } p^\alpha, \\ 0 & \text{otherwise.} \end{cases}$$

*Proof.* First note that any $0 < x < p^\alpha$, $p \nmid x$, can be uniquely expressed as $x = i + jp^{\alpha-1}$ for $0 < i < p^{\alpha-1}$, $0 \le j < p$ with $p \nmid i$. Thus

$$\begin{aligned} S(a, b, \chi, p^\alpha) &= \sum_{i=1,\, p\nmid i}^{p^{\alpha-1}} \sum_{j=0}^{p-1} \chi(i + jp^{\alpha-1})^{a(i+jp^{\alpha-1})} \zeta_{p^\alpha}^{b(i+jp^{\alpha-1})} \\ &= \sum_{i=1,\, p\nmid i}^{p^{\alpha-1}} \chi(i)^{ai} \zeta_{p^\alpha}^{bi} \sum_{j=0}^{p-1} \chi(1 + \bar{i}jp^{\alpha-1})^{ai}, \end{aligned}$$

where $\bar{i}$ denotes the multiplicative inverse of $i$ modulo $p^\alpha$. Since we have $\chi(1 + \bar{i}jp^{\alpha-1})^{ai} = \zeta_p^{\lambda \bar{i} j}$ for some integer $\lambda$,

$$\sum_{j=0}^{p-1} \chi(1 + \bar{i}jp^{\alpha-1})^{ai} = \sum_{j=0}^{p-1} \zeta_p^{aj\lambda} = \begin{cases} 0 & \text{if } a\lambda \not\equiv 0 \pmod{p}, \\ p & \text{if } a\lambda \equiv 0 \pmod{p}. \end{cases}$$

If $a \equiv 0 \pmod{p}$ one finds $S(a, b, \chi, p^\alpha) = pS(a/p, b/p, \chi^p, p^{\alpha-1})$. If $\lambda \equiv 0 \pmod{p}$ then $\chi$ is imprimitive and may be defined modulo $p^{\alpha-1}$, which yields $S(a, b, \chi, p^\alpha) = pS(a, b/p, \chi, p^{\alpha-1})$. In the remaining cases $S(a, b, \chi, p^\alpha) = 0$.

In view of the above observations, one may assume $b \not\equiv 0 \pmod p$ in (2) with $\chi$ primitive modulo $p^\alpha$ for $\alpha > 1$. I will show that such a non-zero sum (2) is up to conjugacy just

$$p^{\alpha/2}\sum_{x\in H}\zeta_q^x \quad \text{or} \quad \left(\frac{-2}{p}\right)p^{(\alpha-1)/2}i^*\sqrt{p}\sum_{x\in H}\left(\frac{x}{p}\right)\zeta_q^x \tag{3}$$

according as $\alpha$ is even or odd when $p$ is odd, where $H$ is the group of $(p-1)$-roots of unity modulo $q$. For $p = 2$ it is a conjugate of

$$2^{\alpha/2}2i\sin\frac{2\pi}{q} \quad \text{or} \quad 2^{\alpha/2}2\cos\frac{2\pi}{q}, \tag{4}$$

of algebraic degree $2^{\alpha-2}$ with minimal polynomial easy to determine (see [7], for instance). The sum (3) is an integer multiple of a classical Gaussian period or a quadratic twist of such of algebraic degree $p^{\alpha-1}$, whose minimal polynomial has recently been studied in [8]. In either case, the expressions (3) and (4) lead to a bound

$$|S(a,b,\chi,q)| \le (p-1)\sqrt{q} \quad \text{or} \quad 2\sqrt{q}$$

according as $q$ is odd or even. This bound is of the same order of magnitude obtained by Cochrane [3] for sums of the form $\sum \chi(g(x))\zeta_q^{f(x)}$ for rational functions $f(x)$ and $g(x)$ with integer coefficients, when the associated critical point congruence has $p-1$ zeros, all of multiplicity one (chiefly, Theorems 1.1 and 6.1 when $t = 0$ in [3]).

My principal tool in determining the explicit values for (2) is an adaptation of the classical method of Salié [12] for Kloosterman sums, together with basic facts about the $p$-adic exponential and logarithm functions and primitive characters. The case for odd primes $p$ is treated first, with sums (2) explicitly evaluated in Section 2. The case $p = 2$ is considered separately in Section 3. In the final section of the paper, I explicitly evaluate certain incomplete sums for odd prime powers $q = p^\alpha$ with $\alpha > 1$ and primitive characters $\chi$ modulo $q$ of the form

$$\sum_{x=1,\,p\nmid x}^{\phi(q)/f} \chi(x)^{ax}\zeta_q^{bx}, \qquad a, b \not\equiv 0 \pmod p, \tag{5}$$

with $f = \gcd(a\phi(q)/o(\chi), p-1)$ where $o(\chi)$ is the order of $\chi$. There is a natural extension of the theory developed here for analogous exponential sums defined over residue rings of algebraic integers. This generalization will appear in a sequel.

It is an interesting exercise to adapt Cochrane's methods in [3] to the situation here to evaluate (2) using $p$-adic and algebraic techniques, though the more direct approach I employ here is simpler and particularly convenient for evaluating the incomplete sums in (5). I include a discussion of the relationship, at least for odd primes $p$, at the end of Section 2.

Lastly, I should mention that my initial interest in the sums (2) and (5) arose from the problem of determining hyper-Kloosterman sums. The results here are applied in [9] to explicitly evaluate the multi-dimensional Kloosterman sums, thus generalizing the classical result of Salié [12] for prime powers in the one-dimensional case.

**2. Evaluation of $\sum \chi(x)^{ax}\zeta_q^{bx}$ for $q$ odd.** Here I consider the sums in (2) with $b \not\equiv 0 \pmod p$ when $q = p^\alpha$ is odd and $\alpha > 1$. Fix a character $\psi$ modulo $q$ which generates the group of all numerical characters defined modulo $q$ and is *normalized* so that

$$\begin{aligned} \psi(1+p^s) &= \zeta_{p^s}^{-1} && \text{for } \alpha = 2s, \\ \psi\left(1+p^s+\left(\frac{p+1}{2}\right)p^{2s}\right) &= \zeta_{p^{s+1}}^{-1} && \text{for } \alpha = 2s+1. \end{aligned} \tag{6}$$

Set $s' = s$ or $s+1$ according as $\alpha$ is even or odd. Any given character $\chi$ defined modulo $q$ equals $\psi^v$ for some integer $v$, $0 \le v < \phi(q)$. Such a character $\chi$ is itself *normalized* if and only if $v \equiv 1 \pmod{p^{s'}}$.

Now choose a primitive root $g$ for $q$, and let $k$ be the least positive integer satisfying $\psi(g) = \zeta_{\phi(q)}^k$. The following lemma and proposition will be crucial in the determination of the sums (2). Here the multiplicative inverse of any $x$ in $\mathbb{Z}_q^*$ will be denoted by $\overline{x}$. The Legendre symbol is denoted by $\left(\frac{-}{p}\right)$ and $i^* = i^{(p-1)^2/4}$.

LEMMA 1. *With a primitive root $g$ for $q$ chosen as above*,

$$g^{(p-1)p^{s-1}y} \equiv \begin{cases} 1 - ykp^s \pmod q & \text{if } \alpha = 2s, \\ 1 - ykp^s - ky(p-ky)p^{2s}/2 \pmod q & \text{if } \alpha = 2s+1, \end{cases}$$

*for any integer $y$.*

*Proof.* I consider the case $\alpha = 2s$ first. By the choice of $\psi$ and $g$, $\psi(g^{-(p-1)p^{s-1}\overline{k}}) = \zeta_{p^s}^{-1}$. But $\psi$ is an isomorphism between $\mathbb{Z}_q^*$ and the group of $\phi(q)$-roots of unity, so from (6), $g^{-(p-1)p^{s-1}\overline{k}} \equiv 1 + p^s \pmod q$. From the $p$-adic negative binomial series

$$(1+x)^{-r} = \sum_{n=0}^{\infty} (-1)^n \binom{n+r-1}{r-1} x^n \tag{7}$$

one finds for any integer $y$ that

$$g^{(p-1)p^{s-1}y} = g^{-(p-1)p^{s-1}\overline{k}(-ky)} \equiv (1+p^s)^{-ky} \equiv 1 - kyp^s \pmod q.$$

Next consider the case $\alpha = 2s+1 > 1$. Arguing as above, one finds from (6) that

$$g^{-(p-1)p^{s-1}\bar{k}} \equiv 1 + p^s + \frac{p+1}{2}\,p^{2s} \pmod{q}.$$

Using (7) one now finds $g^{(p-1)p^{s-1}y} = g^{-(p-1)p^{s-1}\bar{k}(-ky)}$ congruent modulo $q$ to

$$\left(1 + p^s + \frac{p+1}{2}\,p^{2s}\right)^{-ky} \equiv 1 - kyp^s - ky\,\frac{p-ky}{2}\,p^{2s}.$$

The proof of the lemma is now complete.

Now consider the congruence

$$pkvt \equiv v - 1 \pmod{p^{s'}}. \tag{8}$$

When $v \equiv 1 \pmod{p}$ let $t$ be its unique solution with $0 \le t < p^{s'-1}$, and set

$$t(v) = g^{(p-1)t}(1 + pkvt). \tag{9}$$

With notation as above,

PROPOSITION 3. *For $\alpha \ge 2$,*

$$\sum_{j=0}^{p^{\alpha-1}-1} \zeta_q^{g^{(p-1)j}(1+pkvj)} = \begin{cases} p^{\alpha/2}\zeta_q^{t(v)} & \text{if } \alpha \text{ is even and } v \equiv 1 \pmod{p}, \\ \left(\frac{-2}{p}\right) i^* \sqrt{p}\, p^{(\alpha-1)/2}\zeta_q^{t(v)} & \text{if } \alpha \text{ is odd and } v \equiv 1 \pmod{p}, \\ 0 & \text{if } v \not\equiv 1 \pmod{p}, \end{cases}$$

*with $t(v)$ as given in* (9).

*Proof.* Noting that one may uniquely write each $j$ in the summation as $j = t + ip^{s'-1}$ for $0 \le t < p^{s'-1}$, $0 \le i < p^s$, one has

$$\begin{aligned} \sum_{j=0}^{p^{\alpha-1}-1} \zeta_q^{g^{(p-1)j}(1+pkvj)} &= \sum_{t=0}^{p^{s'-1}-1} \sum_{i=0}^{p^s-1} \zeta_q^{g^{(p-1)(t+ip^{s'-1})}(1+pkvt+p^{s'}kvi)} \\ &= \sum_{t=0}^{p^{s'-1}-1} \zeta_q^{g^{(p-1)t}(1+pkvt)} \sum_{i=0}^{p^s-1} \zeta_q^{g^{(p-1)t}(kp^{s'}i)(v-1-pkvt)} \end{aligned}$$

since

$$\begin{aligned} g^{(p-1)p^{s'-1}i}(1 + pkvt + p^{s'}kvi) &\equiv (1 - ikp^{s'})(1 + pkvt + p^{s'}kvi) \\ &\equiv 1 + pvkt + ikp^{s'}(v - 1 - pkvt) \pmod{q} \end{aligned}$$

from Lemma 1. But

$$(10)\qquad \sum_{i=0}^{p^s-1} \zeta_{p^s}^{g^{(p-1)t}ki(v-1-pkvt)} = \begin{cases} p^s & \text{if } pkvt \equiv v-1 \pmod{p^s}, \\ 0 & \text{otherwise.} \end{cases}$$

Since $pkvt \equiv v-1 \pmod{p^s}$ is solvable iff $v \equiv 1 \pmod{p}$, the double sum above is zero when $v \not\equiv 1 \pmod{p}$. When $\alpha$ is even and $v \equiv 1 \pmod{p}$, the double sum above reduces to the single term $p^s \zeta_q^{g^{(p-1)t}(1+pkvt)}$, where $t$ is the solution specified in (9). When $\alpha$ is odd and $v \equiv 1 \pmod{p}$, the congruence $pkvt \equiv v-1 \pmod{p^s}$ has $p$ solutions, namely $t + yp^{s-1}$ $(0 \le y < p)$, where $t$ is the solution specified in (9). In this case the double sum becomes

$$(11)\qquad p^s \sum_{y=0}^{p-1} \zeta_q^{g^{(p-1)(t+yp^{s-1})}(1+pkvt+p^skvy)},$$

which equals

$$p^s \zeta_q^{g^{(p-1)t}(1+pkvt)} \sum_{y=0}^{p-1} \zeta_p^{-k^2y^2/2},$$

since by Lemma 1,

$$\begin{aligned} g^{(p-1)p^{s-1}y}&(1+pkvt+p^skvy) \\ &\equiv \left(1 - kyp^s - ky\,\frac{p-ky}{2}\,p^{2s}\right)(1+pkvt+p^skvy) \\ &\equiv 1 + pkvt + p^{2s}\left(\frac{v-1-pkvt}{p^s}\,ky\right) + p^{2s}\left(\frac{1-2v}{2}\,k^2y^2\right) \\ &\equiv 1 + pkvt - p^{2s}k^2y^2/2 \pmod{q}. \end{aligned}$$

It follows from the standard evaluation $\sum_{y=0}^{p-1} \zeta_p^{dy^2} = \left(\frac{d}{p}\right) i^* \sqrt{p}$ for quadratic Gauss sums that the sum (11) equals

$$p^s \zeta_q^{g^{(p-1)t}(1+pkvt)} \left(\frac{-2}{p}\right) i^* \sqrt{p}.$$

Thus, the result of the proposition holds in all the cases.

I note that the sum in Proposition 3 ordinarily depends on the choice of generator $g$ and the value of $v$ modulo $p^{\alpha-1}$. However, the special case $v \equiv 1 \pmod{p^{s'}}$ is exceptional. In this case $t = 0$ in (9) so by Proposition 3,

Corollary 1. *For $\alpha > 1$ and $v \equiv 1 \pmod{p^{s'}}$,*

$$\sum_{j=0}^{p^{\alpha-1}-1} \zeta_q^{g^{(p-1)j}(1+pkvj)} = \begin{cases} \sqrt{q}\,\zeta_q & \text{if } \alpha \text{ is even}, \\ \left(\frac{-2}{p}\right) i^* \sqrt{q}\,\zeta_q & \text{if } \alpha \text{ is odd}, \end{cases}$$

*independent of the choice of generator $g$.*

Here are a couple of examples to illustrate Proposition 3 and the corollary above.

EXAMPLE 1. Consider $q = 27$ in Proposition 3 with primitive root $g = 2$ and normalized character $\psi$ in (6) satisfying $\psi(2) = \zeta_{18}^5$ with $k = 5$. One finds for $v \equiv 1 \pmod 3$ that

$$\sum_{j=0}^{8} \zeta_{27}^{4^j(1+15vj)} = 3i\sqrt{3}\,\zeta_{27}^{t(v)}$$

with $t(v)$ given by

| $v$ | 1 | 4 | 7 |
|---|---|---|---|
| $t(v)$ | 1 | 19 | 19 |

It suffices to determine $t(v)$ for $v \pmod 9$ here by the remark above. For this example the values of $t(v)$ happen to be independent of the choice of generator $g$ since $t(4) = t(7)$ in view of Corollary 1.

With $q = 81$ in Proposition 3 and normalized character $\psi$ in (6) satisfying $\psi(2) = \zeta_{54}^{11}$ with $k = 11$, one finds for $v \equiv 1 \pmod 3$ that

$$\sum_{j=0}^{26} \zeta_{81}^{4^j(1+33vj)} = 81\zeta_{81}^{t(v)}$$

with $t(v)$ given by

| $v$ | 1 | 4 | 7 | 10 | 13 | 16 | 19 | 22 | 25 |
|---|---|---|---|---|---|---|---|---|---|
| $t(v)$ | 1 | 28 | 37 | 1 | 55 | 10 | 1 | 1 | 64 |

EXAMPLE 2. Consider $q = 343$ in Proposition 3 with primitive root $g = 3$ and normalized character $\psi$ in (6) satisfying $\psi(3) = \zeta_{294}^{71}$ with $k = 71$. One finds for $v \equiv 1 \pmod 7$ here that

$$\sum_{j=0}^{48} \zeta_{343}^{3^{6j}(1+154vj)} = -7i\sqrt{7}\,\zeta_{343}^{t(v)}$$

with $t(v)$ given by

| $v$ | 1 | 8 | 15 | 22 | 29 | 36 | 43 |
|---|---|---|---|---|---|---|---|
| $t(v)$ | 1 | 197 | 99 | 50 | 50 | 99 | 197 |

In the examples above the values $t(v)$ all satisfy $t(v) \equiv 1 \pmod{p^2}$, a relation that is readily confirmed to hold in general when $p$ is odd.

I am ready to state the main result concerning the sums (2).

THEOREM 1. *Suppose $\chi = \psi^v$ in (2) where $a \equiv 0 \pmod{p-1}$ and $b \not\equiv 0 \pmod p$ with $\alpha > 1$. If $av \not\equiv b \pmod p$ then $S(a, b, \chi, q) = 0$ else*

$$S(a,b,\chi,q) = \begin{cases} p^{\alpha/2} \sum_{x\in H} \zeta_q^{bxg^{(p-1)t}(1+pa\bar{b}vkt)} & \text{if } \alpha \text{ is even,} \\ \left(\frac{-2}{p}\right) p^{(\alpha-1)/2} i^* \sqrt{p} \sum_{x\in H} \left(\frac{bx}{p}\right) \zeta_q^{bxg^{(p-1)t}(1+pa\bar{b}vkt)} & \text{if } \alpha \text{ is odd.} \end{cases}$$

*Here $H$ is the group of $(p-1)$-roots of unity modulo $q$, and $t$ satisfies*

$$pkavt \equiv av - b \pmod{p^{s'}} \quad \text{with } 0 \le t < p^{s'-1}$$

*when $av \equiv b \pmod{p}$.*

*Proof.* First note that since $o(\chi^a) \mid q$,

$$\sum_{x \in \mathbb{Z}_q^*} \psi^v(x)^{ax} \zeta_q^{bx} = \sum_{w=0}^{\phi(q)-1} \psi^v(g^w)^{ag^w} \zeta_q^{bg^w},$$

which equals

$$\sum_{i=0}^{p-2} \sum_{j=0}^{p^{\alpha-1}-1} \psi^v(g^{ip^{\alpha-1}+j(p-1)})^{ag^{ip^{\alpha-1}+j(p-1)}} \zeta_q^{bg^{ip^{\alpha-1}+j(p-1)}},$$

where each $w$ is uniquely expressed modulo $\phi(q)$ as $w = ip^{\alpha-1} + j(p-1)$ with $0 \le i < p-1$, $0 \le j < p^{\alpha-1}$. This last sum in turn becomes

$$\sum_{i=0}^{p-2} \sum_{j=0}^{p^{\alpha-1}-1} \psi^v(g^{ip^{\alpha-1}})^{ag^{ip^{\alpha-1}} g^{j(p-1)}} \psi^v(g^{(p-1)j})^{ag^{ip^{\alpha-1}} g^{j(p-1)}} \zeta_q^{bg^{ip^{\alpha-1}} g^{(p-1)j}}$$

$$= \sum_{i=0}^{p-2} \sum_{j=0}^{p^{\alpha-1}-1} \zeta_q^{g^{(p-1)j}(1+pka\bar{b}vj)bg^{ip^{\alpha-1}}} = \sum_{x \in H} \sum_{j=0}^{p^{\alpha-1}-1} \zeta_q^{bxg^{(p-1)j}(1+pka\bar{b}vj)},$$

since $\psi(g^{p^{\alpha-1}})^a = 1$ as $g^{p^{\alpha-1}}$ has order $p-1$ and generates $H$. Thus from Proposition 3 with $a\bar{b}v$ replacing $v$, the sum $S(a,b,\chi,q)$ equals 0 if $av \not\equiv b \pmod{p}$, and otherwise

$$S(a,b,\chi,q) = \begin{cases} \sum_{x \in H} p^{\alpha/2} \zeta_q^{bxt(a\bar{b}v)} & \text{if } \alpha \text{ is even,} \\ \sum_{x \in H} \left(\frac{-2}{p}\right) p^{(\alpha-1)/2} i^* \sqrt{p} \left(\frac{bx}{p}\right) \zeta_q^{bxt(a\bar{b}v)} & \text{if } \alpha \text{ is odd,} \end{cases}$$

when $av \equiv b \pmod{p}$ in terms of the function $t()$ in (9). The statement of the theorem now follows.

The special case where $av \equiv b \pmod{p^{s'}}$ again warrants separate consideration.

Corollary 2. *For any numerical character $\chi = \psi^v$ with $av \equiv b \pmod{p^{s'}}$ in (2), where $a \equiv 0 \pmod{p-1}$, $b \not\equiv 0 \pmod{p}$ and $\alpha > 1$,*

$$S(a,b,\chi,q) = \begin{cases} p^{\alpha/2} \sum_{x \in H} \zeta_q^{bx} & \text{if } \alpha \text{ is even,} \\ \left(\frac{-2}{p}\right) p^{(\alpha-1)/2} i^* \sqrt{p} \sum_{x \in H} \left(\frac{bx}{p}\right) \zeta_q^{bx} & \text{if } \alpha \text{ is odd,} \end{cases}$$

*independent of the choice of normalized character $\psi$ in (6).*

*Proof.* The above follows readily from Theorem 1 and Corollary 1 upon replacing $v$ by $a\bar{b}v$ and noting that $t = 0$ in Theorem 1.

It is worth noting the connection here with the general mixed exponential sums of the form $\sum \chi(g(x))\zeta_q^{f(x)}$ recently studied by T. Cochrane and Z. Zheng [3–5] for prime powers $q = p^\alpha$ $(\alpha > 1)$. In [3] Cochrane considers the case $f(x)$ and $g(x)$ are rational functions with integer entries, and shows how to explicitly evaluate such a sum when its associated critical point congruence has no multiple zeros modulo $p$. For appropriately chosen Taylor series expansions for $f(x)$ and $g(x)$ he extends the classic method of Salié to determine the contribution to the sum $\sum \chi(g(x))\zeta_q^{f(x)}$ from each zero of the critical point congruence. Cochrane and Zheng's techniques will extend to more general settings, where $f(x)$ and $g(x)$ have nice enough $p$-adic analytic properties. Such an adaptation is possible here, which I shall sketch below, but first I make some preliminary remarks about the $p$-adic logarithm and exponential functions.

Let $\mathbb{Q}_p$ denote the field of $p$-adic numbers, $\mathbb{O}_p$ the ring of $p$-adic integers and $\mathbb{U}_p = \{x \in \mathbb{O}_p \mid x \equiv 1 \pmod p\}$ the group of principal units. Any character $\chi$ modulo $q$ extends to $\mathbb{O}_p$ in the natural way; namely $\chi(u) = \chi(\widehat{u})$ where $\widehat{u}$ denotes the residue class of $u$ modulo $q$, and similarly for $\zeta_q^u = \exp(2\pi i\widehat{u}/q)$. The $p$-adic logarithm and exponential functions given by

$$\log(1+pu) = \sum_{j=1}^{\infty}(-1)^{j+1}\frac{(pu)^j}{j} \quad \text{and} \quad e^{pu} = \sum_{j=0}^{\infty}\frac{(pu)^j}{j!} \tag{12}$$

are analytic on $\mathbb{O}_p$ and satisfy the identity $e^{\log(1+pu)} = 1 + pu$ for $u \in \mathbb{O}_p$. Corresponding to the primitive root $g$ for $q$ chosen before, let $R$ be the $p$-adic unit $R = \frac{1}{p}\log g^{p-1}$. One defines the exponential function

$$z = g^{(p-1)t} = e^{Rpt} \qquad (t \in \mathbb{O}_p) \tag{13}$$

which maps $\mathbb{O}_p$ isomorphically onto $\mathbb{U}_p$. With respect to the filtration $\mathbb{U}_p^{(i)} = \{u \in \mathbb{U}_p \mid u \equiv 1 \pmod{p^i}\}$ $(i > 0)$ of the principal units, the image $z(p^{\gamma-1}\mathbb{O}_p)$ equals $\mathbb{U}_p^{(\gamma)}$ for any positive integer $\gamma$. The inverse map for (13) is

$$t = R^{-1}p^{-1}\log z \qquad (z \in \mathbb{U}_p). \tag{14}$$

With $\chi = \psi^v$ here in terms of the normalized character $\psi$ chosen in (6), one finds (chiefly Lemma 2.1 in [3]) that

$$\chi(1+pu) = \zeta_q^{\bar{R}kv\log(1+pu)} \qquad (u \in \mathbb{O}_p). \tag{15}$$

Since $\psi$ satisfies (6) one readily sees from (15) that $k \equiv -R \pmod{p^{s'}}$ with $q = 27$ being the only exception.

For the application here $f(x) = bx$ and $g(x) = \exp(x\log x^a)$ are both defined for $\mathbb{U}_p$ since $a \equiv 0 \pmod{p-1}$. Relying on (15) and the power series expansions (12), one can show that

$$\chi(x+p^{s'}y)^{a(x+p^{s'}y)} = \chi(x)^{ax}\zeta_q^{\bar{R}kv(\log x^a+a)yp^{s'}}$$

for any $y \in \mathbb{O}_p$, analogous to relation (3.5) in [3]. The associated critical point congruence may be expressed as

$$W(x) := Rb + kv\log x^a + kav \equiv 0 \ (\mathrm{mod}\, p^{s'}), \qquad x \not\equiv 0 \ (\mathrm{mod}\, p),$$

in place of $C(x)/g(x) = Rf'(x) + kvg'(x)/g(x) \equiv 0$ there. Since $\psi$ is normalized, $R$ may be replaced by $-k$ in view of the comments above (except for $q = 27$), so the critical point congruence becomes

$$(16) \qquad W(x) :\equiv k(av-b) + kv\log x^a \equiv 0 \ (\mathrm{mod}\, p^{s'}), \qquad x \not\equiv 0 \ (\mathrm{mod}\, p).$$

But $x^a \equiv 1 \ (\mathrm{mod}\, p)$ so $W(x) \equiv 0 \ (\mathrm{mod}\, p)$ is solvable if and only if $av \equiv b \ (\mathrm{mod}\, p)$, and then for any $x \not\equiv 0 \ (\mathrm{mod}\, p)$. Additionally $W'(x) \equiv kva/x \not\equiv 0 \ (\mathrm{mod}\, p)$ so each zero of $W(x) \equiv 0 \ (\mathrm{mod}\, p)$ is simple.

To find the lift $x^*$ for $x \equiv 1 \ (\mathrm{mod}\, p)$ in (16) one may algebraically solve for $x^*$ making use of (13) and (14). Indeed, from (16), one has $\log x^* \equiv -(av-b)/av \ (\mathrm{mod}\, p^{s'})$ or $t \equiv \overline{R}p^{-1}\log x^* \equiv (av-b)/pkav \ (\mathrm{mod}\, p^{s'-1})$ since $k \equiv -R \ (\mathrm{mod}\, p^{s'})$. Thus $x^* \equiv g^{(p-1)t}$, where $t \equiv (av-b)/pkav \ (\mathrm{mod}\, p^{s'-1})$, is the lift for $x \equiv 1 \ (\mathrm{mod}\, p)$ with the contribution

$$S_1 = \begin{cases} p^{\alpha/2}\zeta_q^{bg^{(p-1)t}(1+pka\bar{b}vt)} & \text{if } \alpha \text{ is even,} \\ p^{(\alpha-1)/2}i^*\sqrt{p}\left(\frac{-2b}{p}\right)\zeta_q^{bg^{(p-1)t}(1+pba\bar{b}vt)} & \text{if } \alpha \text{ is odd} \end{cases}$$

from Theorem 1.1 in [3] since

$$\chi(g^{(p-1)tag^{(p-1)t}})\zeta_q^{bg^{(p-1)t}} = \zeta_{p^{\alpha-1}(p-1)}^{k(p-1)avtg^{(p-1)t}}\zeta_q^{bg^{(p-1)t}} = \zeta_q^{bg^{(p-1)t}(1+pkav\bar{b}t)}$$

and $-2kW'(1) \equiv -2b \ (\mathrm{mod}\, p)$.

To find lifts for the remaining solutions of $W(x) \equiv 0 \ (\mathrm{mod}\, p)$, note that the group $H$ of $(p-1)$-roots of unity modulo $q$ is isomorphic to $\mathbb{Z}_p^*$ so one may as well take $H$ as the solution set of the critical point congruence (16) modulo $p$. But now for each $\mu \in H$, $\mu x^*$ is a lift of $\mu$ satisfying (16) since $\mu^a \equiv 1 \ (\mathrm{mod}\, p^{s'})$. Moreover, $\chi(\mu x^*)^{av\mu x^*}\zeta_q^{b\mu x^*} = \chi(x^*)^{avx^*\mu}\zeta_q^{bx^*\mu}$ with $-2kW'(\mu) \equiv -2b/\mu \ (\mathrm{mod}\, p)$ so the contribution due to $\mu$ is $S_\mu = \sigma_\mu(S_1)$, where $\sigma_\mu$ is the automorphism of $\mathbb{Q}(\zeta_q)/\mathbb{Q}$ satisfying $\sigma_\mu(\zeta_q) = \zeta_q^\mu$. Thus $\sum_{x\in\mathbb{Z}_q^*}\chi(x)^{ax}\zeta_q^{bx} = \sum_{\mu\in H} S_\mu$ yielding the expressions appearing in Theorem 1. A slight modification of the argument above yields the same result in the exceptional case $q = 27$.

**3. Evaluation of $\sum \chi(x)^{ax}\zeta_q^{bx}$ for $q = 2^\alpha$.** Here I consider the sums in (2) when $q = 2^\alpha$ with $b$ odd and $\alpha > 1$. It is straightforward to compute these sums for $q = 4$ or 8. Here $\xi$ denotes the quadratic character $\xi(x) =$

$(-1)^{(x-1)/2}$, and $\left(\frac{2}{x}\right)$ and $\left(\frac{-2}{x}\right)$ the usual Kronecker symbols associated with $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{-2})$, respectively.

PROPOSITION 4. *For $b$ odd*

$$\text{(i)}\qquad S(a,b,\chi,4)=\begin{cases}0 & \text{if } \chi^a=1,\\ 2i^b & \text{if } \chi^a\neq 1,\end{cases}$$

$$\text{(ii)}\qquad S(a,b,\chi,8)=\begin{cases}0 & \text{if } \chi^a=1 \text{ or } \xi,\\ \left(\frac{2}{b}\right)2\sqrt{2} & \text{if } \chi(x)=\left(\frac{2}{x}\right) \text{ and } a \text{ is odd},\\ \left(\frac{2}{x}\right)2i^b\sqrt{2} & \text{if } \chi(x)=\left(\frac{-2}{x}\right) \text{ and } a \text{ is odd}.\end{cases}$$

The above result is readily obtained by direct calculation from (2).

I now assume $\alpha > 3$ throughout the remainder of this section. Fix a numerical character $\psi$ modulo $q$ which generates the group of all *even* numerical characters defined modulo $q$ and is *normalized* so that

$$\psi(1+2^s)=\zeta_{2^s}^{-1} \qquad \text{for } \alpha=2s,\ s\geq 2, \tag{17}$$
$$\psi(1+2^s+2^{2s-1})=\zeta_{2^{s+1}}^{-1} \qquad \text{for } \alpha=2s+1,\ s\geq 2.$$

Set $s'=s$ or $s+1$ again as $\alpha$ is even or odd. Note that $\psi$ has order $2^{\alpha-2}$ and that any given numerical character $\chi$ defined modulo $q$ equals $\psi^v$ or $\xi\psi^v$ for some integer $v$, $0\leq v<2^{\alpha-2}$. Additionally one sees that such a character $\chi$ is itself *normalized* if and only if $v\equiv 1 \pmod{2^{s'}}$.

Next choose a generator $g\equiv 1 \pmod 4$ for the subgroup $T=\{v\in\mathbb{Z}_{2^\alpha}^* \mid v\equiv 1 \pmod 4\}$ of $\mathbb{Z}_{2^\alpha}^*$, say with the least positive integer $k$ satisfying $\psi(g)=\zeta_{2^{\alpha-2}}^k$.

The following lemma and propositions are the natural analogs of those given at the beginning of Section 2 for the situation at hand.

LEMMA 2. *With generator $g$ chosen as above*

$$g^{2^{s-2}y}\equiv\begin{cases}1-yk2^s \pmod q & \text{if } \alpha=2s,\\ 1-yk2^s+(yk)^2 2^{2s-1} \pmod q & \text{if } \alpha=2s+1,\end{cases}$$

*for any integer $y$.*

*Proof.* In case $\alpha=2s$ one has $\psi(g^{-\bar{k}2^{s-2}})=\zeta_{2^s}^{-1}$ by the choice of $\psi$ and $g$. Now $\psi$ is an isomorphism between $T$ and the group of $2^{\alpha-2}$-roots of unity, so from (17),

$$g^{-\bar{k}2^{s-2}}\equiv 1+2^s \pmod q.$$

In particular using (7) one finds that

$$g^{2^{s-2}y}\equiv g^{-\bar{k}2^{s-2}(-ky)}\equiv(1+2^s)^{-ky}\equiv 1-ky2^s \pmod q.$$

In the alternative case $\alpha=2s+1$, one finds similarly that

$$g^{-\bar{k}2^{s-2}}\equiv 1+2^s+2^{2s-1} \pmod q.$$

Using (7) again, one has $g^{2^{s-2}y} = g^{-\bar{k}2^{s-2}(-ky)} \equiv (1 + 2^s + 2^{2s-1})^{-ky}$ or $-ky(2^s + 2^{2s-1}) + \frac{ky(ky+1)}{2}(2^s + 2^{2s-1})^2 \equiv 1 - ky2^s + (ky)^2 2^{2s-1} \pmod{q}$.

Now consider the congruence

$$4kvt \equiv v - 1 \pmod{2^{s'}}. \tag{18}$$

When $v \equiv 1 \pmod 4$ let $t$ be its unique solution with $0 \le t < 2^{s'-2}$, and set

$$t(v) = \begin{cases} g^t(1 + 4kvt) & \text{if } \alpha \text{ is even,} \\ g^t(1 + 4kvt + (1 - 2(-1)^t)2^{\alpha-3}) & \text{if } \alpha \text{ is odd.} \end{cases} \tag{19}$$

With notation as above, we have

Proposition 5. *For $\alpha > 3$ and $v \equiv 1 \pmod 4$,*

$$\sum_{j=0}^{2^{\alpha-4}-1} \zeta_{2^\alpha}^{g^j(1+4kvj)} = 2^{(\alpha-4)/2} \zeta_{2^\alpha}^{t(v)}$$

*with $t(v)$ as given in* (19).

*Proof.* When $\alpha = 4$, the sum consists of the single term $\zeta_{16}$ with $t = 0$ in (19) so the formula holds. When $\alpha = 5$, the sum equals $\zeta_{32} + \zeta_{32}^{g(1+4kv)}$ with $t = 0$ or 1 according as $v \equiv 1$ or $5 \pmod 8$. A straightforward computation shows this sum equals $\sqrt{2}\,\zeta_{32}^{-3}$ or $\sqrt{2}\,\zeta_{32}^{5}$ respectively, independent of the choice of $g$, so the result of the proposition follows for $\alpha = 5$. Now assume $\alpha > 5$ and write $j = t + i2^{s'-2}$ for $0 \le i < 2^{s-2}$ and $0 \le t < 2^{s'-2}$. Then

$$\begin{aligned} \sum_{j=0}^{2^{\alpha-4}-1} \zeta_q^{g^j(1+4kvj)} &= \sum_{t=0}^{2^{s'-2}-1} \sum_{i=0}^{2^{s-2}-1} \zeta_q^{g^{t+i2^{s'-2}}(1+4kvt+2^{s'}kvi)} \\ &= \sum_{t=0}^{2^{s'-2}-1} \zeta_q^{g^t(1+4kvt)} \sum_{i=0}^{2^{s-2}-1} \zeta_{2^s}^{g^t ki(v-1-4kvt)} \end{aligned}$$

since

$$\begin{aligned} g^{i2^{s'-2}}(1 + 4kvt + 2^{s'}kvi) &\equiv (1 - ik2^{s'})(1 + 4kvt + 2^{s'}kvi) \\ &\equiv 1 + 4kvt + ik2^{s'}(v - 1 - 4kvt) \pmod{q} \end{aligned}$$

from Lemma 2. But

$$\sum_{i=0}^{2^{s-2}-1} \zeta_{2^{s-2}}^{g^t ki((v-1)/4-kvt)} \equiv \begin{cases} 2^{s-2} & \text{if } (v-1)/4 \equiv kvt \pmod{2^{s-2}}, \\ 0 & \text{otherwise.} \end{cases} \tag{20}$$

For $\alpha$ even, the double sum above reduces to the single term $2^{s-2}\zeta_q^{g^t(1+4kvt)}$, where $t$ is the solution specified in (19). For $\alpha$ odd, the double sum becomes

$$2^{s-2}(\zeta_q^{g^t(1+4kvt)} + \zeta_q^{g^{t+2^{s-2}}(1+4kvt+2^s kv)})$$
$$= 2^{s-2}(\zeta_q^{g^t(1+4kvt)} + \zeta_q^{g^t(1+4kvt+k(v-1)2^s-k^2v2^{2s}-k^2vt2^{s+2}+2^{2s-1})}),$$

where $t$ is the solution specified in (19). Since $g^{2^{s-2}} \equiv 1-k2^s+2^{2s-1} \pmod q$ from Lemma 2 as $k$ is odd, the last expression is seen to equal

$$2^{s-2}\zeta_q^{g^t(1+4kvt-2^{2s-2})}(\zeta_8^{g^t} + \zeta_8^{-g^t}) = \left(\frac{2}{g^t}\right)2^{s-2}\sqrt{2}\,(\zeta_q^{1+4kvt}\zeta_8^{-1})^{g^t}.$$

The result of the proposition now follows as stated for $\alpha$ odd with the expression for $t(v)$ since $g \equiv 5 \pmod 8$. Thus the proof of the proposition is complete.

I note that the sum in Proposition 5 ordinarily depends on the choice of generator $g$ for $T$ and value of $v$ modulo $2^{\alpha-2}$. However, the special case $v \equiv 1 \pmod{2^{s'}}$ is exceptional. In this case $t = 0$ in (19) so by Proposition 5,

COROLLARY 3. *For $\alpha > 3$ and $v \equiv 1 \pmod{2^{s'}}$,*

$$\sum_{j=0}^{2^{\alpha-4}-1} \zeta_q^{g^j(1+4kvj)} = \begin{cases} 2^{(\alpha-4)/2}\zeta_q & \text{if } \alpha \text{ is even,} \\ 2^{(\alpha-5)/2}\sqrt{2}\,\zeta_q\zeta_8^{-1} & \text{if } \alpha \text{ is odd,} \end{cases}$$

*independent of the choice of generator $g$ for $T$.*

COROLLARY 4. *For $\alpha > 3$ odd with $v \equiv 1 + 2^s \pmod{2^{s+1}}$,*

$$\sum_{j=0}^{2^{\alpha-4}-1} \zeta_q^{g^j(1+4kvj)} = 2^{(\alpha-5)/2}\sqrt{2}\,\zeta_q\zeta_8,$$

*independent of the choice of generator $g$ for $T$.*

*Proof.* With $v \equiv 1 + 2^s \pmod{2^{s+1}}$ one finds $t = 2^{s-2}$ in (19). Direct computation shows $t(5) = 5$ when $\alpha = 5$. For $\alpha > 5$, $t$ is even so from Lemma 2 and Proposition 5, $t(v)$ is congruent modulo $q$ to

$$g^{2^{s-2}}(1 + 2^s kv - 2^{2s-2}) \equiv (1 - k2^s + 2^{2s-1})(1 + 2^s kv - 2^{2s-2}) \equiv 1 + 2^{2s-2}.$$

This yields the value stated above.

The following example illustrates Proposition 5 and the corollaries above.

EXAMPLE 3. Here I evaluate $t(v)$ in Proposition 5 for $q = 2^\alpha$ with $5 \le \alpha \le 8$, where $g = 5$ has been chosen to generate the subgroup $T$. It suffices to consider only $v \equiv 1 \pmod 4$ and less than $2^{\alpha-2}$.

For $q = 32$ a normalized character $\psi$ in (17) must satisfy $\psi(5) = \zeta_8$ with $k = 1$. From Proposition 5, one obtains

| $v$ | 1 | 5 |
|---|---|---|
| $t(v)$ | $-3$ | 5 |

For $q = 64$, choosing a normalized character $\psi$ in (17) satisfying $\psi(5) = \zeta_{16}^{-3}$ with $k = -3$, one finds from Proposition 5 that

| $v$ | 1 | 5 | 9 | 13 |
|---|---|---|---|---|
| $t(v)$ | 1 | 25 | 1 | −7 |

Choosing a different normalized character $\widehat{\psi}$ in (17) satisfying $\widehat{\psi}(5) = \zeta_{16}^{5}$ with $k = 5$, one finds instead that

| $v$ | 1 | 5 | 9 | 13 |
|---|---|---|---|---|
| $t(v)$ | 1 | −7 | 1 | 25 |

Similarly for $q = 128$ in Proposition 5 and normalized character $\psi$ satisfying $\psi(5) = \zeta_{32}^{1}$ with $k = 1$ one obtains

| $v$ | 1 | 5 | 9 | 13 | 17 | 21 | 25 | 29 |
|---|---|---|---|---|---|---|---|---|
| $t(v)$ | −15 | −39 | 17 | 25 | −15 | 25 | 17 | −39 |

With normalized character $\psi$ satisfying $\psi(5) = \zeta_{64}^{25}$ in (17) for $k = 25$ where $q = 256$, one finds

| $v$ | 1 | 5 | 9 | 13 | 17 | 21 | 25 | 29 | 33 | 37 | 41 | 45 | 49 | 53 | 57 | 61 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $t(v)$ | 1 | −55 | −31 | −55 | 1 | 9 | 97 | 137 | 1 | 73 | −31 | 73 | 1 | 137 | 97 | 9 |

Choosing a different normalized character $\widehat{\psi}$ in (17) satisfying $\widehat{\psi}(5) = \zeta_{64}^{9}$ one finds instead

| $v$ | 1 | 5 | 9 | 13 | 17 | 21 | 25 | 29 | 33 | 37 | 41 | 45 | 49 | 53 | 57 | 61 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $t(v)$ | 1 | 137 | 97 | 9 | 1 | −55 | −31 | −55 | 1 | 9 | 97 | 137 | 1 | 73 | −31 | 73 |

In the examples above the values $t(v)$ all satisfy $t(v) \equiv 1 \pmod 8$, a relation that is readily confirmed to hold here in general.

In addition to the patterns exhibited among the values $t(v)$ in the examples above that are predicted by Corollaries 3 and 4, there are others worth noting which depend on the choice of generator $g$ for $T$ and value $k$ used to determine the normalized generating character $\psi$ in (17). To present them I describe a canonical choice of normalized characters $\psi_\alpha$ modulo $2^\alpha$ satisfying (17) for $\alpha > 3$ corresponding to the generator $g = 5$ for $T$.

Let $\mathbb{Q}_2$ and $\mathbb{O}_2$ denote the field of 2-adic numbers and ring of 2-adic integers, respectively, and consider a character $\chi$ modulo $q$ extended to $\mathbb{O}_2$ as before and similarly for $\zeta_q^u$. The 2-adic logarithmic and exponential functions given by

$$(21)\qquad \log(1+4u) = \sum_{j=1}^{\infty}(-1)^{j-1}(4u)^j/j \quad\text{and}\quad e^{4u} = \sum_{j=0}^{\infty}(4u)^j/j!$$

are analytic on $\mathbb{O}_2$ and satisfy the identity $e^{\log(1+4u)} = 1+4u$. Let $R$ be the 2-adic unit $R = \frac{1}{4}\log 5$. The exponential function

$$z = 5^t = e^{4Rt} \qquad (t \in \mathbb{O}_2)$$

has inverse $t = \frac{1}{4R}\log z$ for $z \equiv 1 \pmod 4$. For any character $\chi = \psi^v$, in terms of the normalized character $\psi$ chosen in (17), one has (chiefly, (6.4) in [3])

$$\chi(1+4u) = \zeta_q^{\bar{R}kv\log(1+4u)} \qquad (u \in \mathbb{O}_2). \tag{22}$$

Now define a sequence of integers $\{k_\alpha\}$ $(\alpha > 3)$ given by the congruences

$$k_\alpha \equiv \begin{cases} -R(1-2^{s-1}) & \text{if } \alpha = 2s \geq 4, \\ -R & \text{if } \alpha = 2s+1 \geq 5 \end{cases} \tag{23}$$

modulo $2^{\alpha-2}$. The characters $\psi_\alpha$ given by

$$\psi_\alpha(5) = \zeta_{2^{\alpha-2}}^{k_\alpha}, \quad \psi_\alpha(-1) = 1 \qquad (\alpha > 3) \tag{24}$$

are seen to be even and normalized modulo $2^\alpha$, and were the ones chosen for $\psi$ in Example 3 for $5 \leq \alpha \leq 8$.

Proposition 6. *Each character $\psi_\alpha$ above is normalized modulo $2^\alpha$.*

*Proof.* From (22) and (24) one has for any $u \in \mathbb{O}_2$,

$$\psi_\alpha(1+4u) = \zeta_q^{\bar{R}k_\alpha \log(1+4u)}.$$

For $\alpha > 3$ odd one finds using (21) that

$$\psi_\alpha(1+2^s+2^{2s-1}) = \zeta_q^{-(2^s+2^{2s-1})+(2^s+2^{2s-1})^2/2-\cdots} = \zeta_{2^{s'}}^{-1}$$

since $k_\alpha \equiv -R \pmod q$. So $\psi_\alpha$ is normalized in this case. For $\alpha > 2$ even one similarly has

$$\psi_\alpha(1+2^s) = \zeta_q^{(2^{s-1}-1)(2^s-2^{2s-1}+2^{3s}/3-\cdots)} = \zeta_q^{2^s(2^{s-1}-1)(1-2^{s-1})} = \zeta_{2^s}^{-1}$$

since $k_\alpha \equiv -R(1-2^{s-1}) \pmod q$. Thus $\psi_\alpha$ is normalized also for $\alpha$ even.

For the choices made in (23) and (24) I find

Corollary 5. *Let $q = 2^\alpha$ with $\alpha = 2s > 4$ and $k \equiv k_\alpha \pmod{2^{s+1}}$ in* (23). *For $v \equiv 1 + 2^{s-1} \pmod{2^{s+1}}$,*

$$\sum_{j=0}^{2^{\alpha-4}-1} \zeta_q^{5^j(1+4kvj)} = \begin{cases} 2^{(\alpha-4)/2}\zeta_q\zeta_8^{-1} & \textit{if } s > 3, \\ -2^{(\alpha-4)/2}\zeta_q\zeta_8^{-1} & \textit{if } s = 3. \end{cases}$$

*For $v \equiv 1 - 2^{s-1} \pmod{2^{s+1}}$ the above sum has the same values but with the alternatives interchanged.*

*Proof.* The choice $v \equiv 1 \pmod{2^{s+1}}$ yields $t = 2^{s-3}$ with $v - 1 - 4kvt \equiv 0 \pmod{2^s}$ in (18). Then $t(v) = g^t(1+4kvt) = 5^{2^{s-3}}(1+2^{s-1}kv)$ is congruent to $(1+2^{s-1}R+2^{2s-3})(1-2^{s-1}R(1-2^{s-1})(1+2^{s-1}))$ modulo $q$ from the 2-adic expansion of $5^{2^{s-3}} = e^{2^{s-1}R}$ in (21). But this expression for $t(v)$ becomes

$$(1+2^{s-1}R+2^{2s-3})(1-R2^{s-1}) \equiv 1-2^{2s-3}+2^{3s-4} \pmod q,$$

which is readily seen to be congruent to $1-2^{2s-3}$ or $1+3\cdot 2^{2s-3}$ according as $s>3$ or $s=3$. The result stated in the corollary now follows. Note that with $v\equiv 1-2^{s-1} \pmod{2^{s+1}}$ instead, a similar computation yields the same values with alternatives interchanged.

Corollary 6. *Let* $q=2^\alpha$ *with* $\alpha=2s>4$ *and* $k\equiv k_\alpha(1+2^s) \pmod{2^{s+1}}$ *in* (23). *For* $v\equiv 1+2^{s-1} \pmod{2^{s+1}}$,

$$\sum_{j=0}^{2^{\alpha-4}-1} \zeta_q^{5^j(1+4kvj)} = \begin{cases} -2^{(\alpha-4)/2}\zeta_q\zeta_8^{-1} & \text{if } s>3, \\ 2^{(\alpha-4)/2}\zeta_q\zeta_8^{-1} & \text{if } s=3. \end{cases}$$

*For* $v\equiv 1-2^{s-1} \pmod{2^{s+1}}$ *the above sum has the same values but with the alternatives interchanged.*

*Proof.* I first note that $1+4kvj$ is invariant modulo $q$ if $k$ and $v$ are replaced by $k(1+2^s)$ and $v(1-2^s)$ respectively in Corollary 5. But $(1+2^{s-1})(1-2^s)\equiv 1-2^{s-1}$ and $(1-2^{s-1})(1-2^s)\equiv 1+2^{s-1}$ modulo $2^{s+1}$ so the result follows from Corollary 5.

Incidentally, the alternative choice of characters in Example 3 for $q=64$ and $q=256$ was made to illustrate Corollaries 5 and 6 above.

I finally remark that if one replaces $-R(1-2^{s-1})$ by $-R(1+2^{s-1})$ in (23) for $\alpha=2s\geq 4$ to define the characters $\psi_\alpha$, then Proposition 6 remains valid, and also Corollaries 5 and 6 but with the alternatives interchanged for the value of the sum $\sum_{j=0}^{2^{\alpha-4}-1}\zeta_q^{5^j(1+4kvj)}$.

I am now ready to state the main result concerning the sums (2) when $p=2$ and $b$ is odd.

Theorem 2. *For* $b$ *odd and* $q=2^\alpha$ *with* $\alpha>3$, *let* $\chi=\psi^v$ *or* $\xi\psi^v$. *If* $av\not\equiv b \pmod 4$ *then* $S(a,b,\chi,q)=0$ *else*

$$S(a,b,\chi,q) = \begin{cases} \left(\frac{2}{b}\right)^\alpha 2\sqrt{q}\cos\left(\frac{2\pi bt(a\bar{b}v)}{q}\right) & \text{if } \chi=\psi^v, \\ \left(\frac{2}{b}\right)^\alpha 2i\sqrt{q}\sin\left(\frac{2\pi bt(a\bar{b}v)}{q}\right) & \text{if } \chi=\xi\psi^v. \end{cases}$$

*Here* $t()$ *is the function given in* (19).

*Proof.* To begin set

$$W(a,b,\chi,q) = \sum_{x\in T}\chi(x)^{ax}\zeta_q^{bx} \tag{25}$$

for any numerical character $\chi$ modulo $q$, where $T$ is the subgroup $\{x \in \mathbb{Z}_q^* \mid x \equiv 1 \pmod 4\}$ of $\mathbb{Z}_q^*$ as before. One has

$$\sum_{x\in\mathbb{Z}_q^*} \chi(x)^{ax}\zeta_q^{bx} = W(a,b,\chi,q) + \chi^a(-1)W(-a,-b,\chi,q)$$

reducing the computations to sums of the form (25) with $\chi$ even, say $\chi = \psi^v$ for some integer $v$. Now $\psi^v(1+2^{\alpha-2})^{a(1+2^{\alpha-2})} = \psi^{av}(1+2^{\alpha-2}) = \zeta_4^{-av}$ since $\psi$ satisfies (17) with $s \geq 2$. In addition, any element of $T$ has a unique representation modulo $q$ as a product $xy$ with $x \in X = \{1, 5, \ldots, 2^{\alpha-2}-3\}$ and $y \in \{1, 1+2^{\alpha-2}, 1+2^{\alpha-1}, 1+3\cdot 2^{\alpha-2}\}$. Thus

$$\begin{aligned} W(a,b,\chi,q) = &\sum_{x\in X}(\psi(x)^{avx}\zeta_q^{bx} + \psi(x(1+2^{\alpha-2}))^{avx(1+2^{\alpha-2})}\zeta_q^{bx(1+2^{\alpha-2})} \\ &+ \psi(x(1+2^{\alpha-1}))^{avx(1+2^{\alpha-1})}\zeta_q^{bx(1+2^{\alpha-1})} \\ &+ \psi(x(1+3\cdot 2^{\alpha-2}))^{avx(1+3\cdot2^{\alpha-2})}\zeta_q^{bx(1+3\cdot 2^{\alpha-2})}) \\ = &\sum_{x\in X}\psi(x)^{avx}\zeta_q^{bx}(1+\psi(1+2^{\alpha-2})^{av}\zeta_4^{b} \\ &+ \psi(1+2^{\alpha-1})^{av}\zeta_4^{2b} + \psi(1+3\cdot 2^{\alpha-2})^{av}\zeta_4^{3b}) \end{aligned}$$

since $x \equiv 1 \pmod 4$. This in turn equals

$$\sum_{x\in X}\psi(x)^{avx}\zeta_q^{bx}(1+\zeta_4^{b-av}+\zeta_4^{2(b-av)}+\zeta_4^{3(b-av)})$$

so

$$W(\psi^v) = \begin{cases} 4\sum_{x\in X}\psi(x)^{avx}\zeta_q^{bx} & \text{if } av \equiv b \pmod 4, \\ 0 & \text{if } av \not\equiv b \pmod 4. \end{cases} \tag{26}$$

Moreover, the value of any term $\psi(x)^{avx}\zeta_q^{bx}$ in $\sum_{x\in X}\psi(x)^{avx}\zeta_q^{bx}$ for $av \equiv b \pmod 4$ depends only on the choice of $x$ modulo $2^{\alpha-2}$. Taking the values $\{g^j \mid 0 \leq j < 2^{\alpha-4}-1\}$ to represent the elements of $X$ modulo $2^{\alpha-2}$, one now obtains

$$\sum_{x\in X}\psi^{avx}(x)\zeta_q^{bx} = \sum_{j=0}^{2^{\alpha-4}-1}\zeta_{2^{\alpha-2}}^{avkjg^j}\zeta_q^{bg^j} = \sum_{j=0}^{2^{\alpha-4}-1}\zeta_q^{bg^j(1+4ka\bar{b}vj)}, \tag{27}$$

just a conjugate of the sum evaluated in Proposition 5. A straightforward computation using Proposition 5 with $v$ replaced by $a\bar{b}v$ yields

$$S(a,b,\chi,q) = \left(\frac{2}{b}\right)^{\alpha}2^{\alpha/2}(\zeta_q^{bt(a\bar{b}v)} + \chi(-1)\zeta_q^{-bt(a\bar{b}v)})$$

in view of (26) above. The expressions for $S(a,b,\chi,q)$ as stated in the theorem immediately follow.

The special case when $av \equiv b \pmod{2^{s'}}$ warrants separate mention.

COROLLARY 7. *For any character $\chi = \psi^v$ or $\chi = \xi\psi^v$ in (2) with $av \equiv b \pmod{2^{s'}}$ when $p = 2$, $b$ is odd and $\alpha > 3$,*

$$S(a,b,\chi,q) = \begin{cases} 2^{\alpha/2}(\zeta_q^b + \chi(-1)\zeta_q^{-b}) & \text{if } \alpha \text{ is even},\\ 2^{(\alpha-1)/2}\sqrt{2}\left(\frac{2}{b}\right)(\zeta_q^{b(1-2^{\alpha-3})} + \chi(-1)\zeta_q^{-b(1-2^{\alpha-3})}) & \text{if } \alpha \text{ is odd}, \end{cases}$$

*independent of the choice of even normalized character $\psi$ in (17).*

The following results treat the special case when $2^{s'-1} \parallel (av - b)$ and are readily deduced from Corollaries 4 and 5, respectively, in view of Theorem 2. The details are left to the reader.

COROLLARY 8. *For any character $\chi = \psi^v$ or $\xi\psi^v$ in (2) with $2^s \parallel (av - b)$, where $b$ is odd and $q = 2^{2s+1} > 8$,*

$$S(a,b,\chi,q) = \left(\frac{2}{b}\right)2^s\sqrt{2}\,(\zeta_q^{b(1+2^{\alpha-3})} + \chi(-1)\zeta_q^{-b(1+2^{\alpha-3})}).$$

COROLLARY 9. *Let $\chi = \psi^v$ or $\xi\psi^v$ in (2) in terms of the canonical characters $\psi_\alpha$ given in (24). If $2^{s-1} \parallel (av - b)$ where $b$ is odd and $q = 2^{2s} > 16$, then*

$$S(a,b,\chi,q) = \begin{cases} \varepsilon 2^s(\zeta_q^{b(1-2^{\alpha-3})} + \chi(-1)\zeta_q^{-b(1-2^{\alpha-3})}) & \text{if } s > 3,\\ -\varepsilon 2^s(\zeta_q^{b(1-2^{\alpha-3})} + \chi(-1)\zeta_q^{-b(1-2^{\alpha-3})}) & \text{if } s = 3. \end{cases}$$

*Here $\varepsilon = \pm 1$ is determined by the congruence $av - b \equiv \varepsilon b 2^{s-1} \pmod{2^{s+1}}$.*

**4. Evaluation of some incomplete sums for primitive characters.** In this section I consider the sums $\sum_{x=1,\, p\nmid x}^{\phi(q)/f} \chi(x)^{ax}\zeta_q^{bx}$ in (5), with $p \nmid b$, $f = \gcd(av, p-1)$ and $\chi$ a primitive character modulo $q$ of the form $\chi = \psi^v$, where $av \equiv b \pmod{p}$ and $\psi$ is normalized as in (6) with $\psi(g) = \zeta_{\phi(q)}^k$ as in Section 2.

The following lemma plays a key role in evaluating these incomplete sums.

LEMMA 3. *For any character $\chi$ modulo $q$ of the form $\chi = \psi^v$, where $av \equiv b \pmod{p}$ with $\psi$ satisfying (6) and $x, y \not\equiv 0 \pmod{p}$,*

$$\chi(x)^{ax}\zeta_q^{bx} = \chi(y)^{ay}\zeta_q^{by} \quad \text{if } x \equiv y \pmod{p^{\alpha-1}(p-1)/f}.$$

*Proof.* First note that since $\psi$ is normalized $\psi(1 + vp^{\alpha-1}) = \zeta_p^{-v}$ for any integer $v$ from (6). Now write $y = x + p^{\alpha-1}(p-1)t/f$ for some integer $t$. Then

$$\chi(y)^{ay} = \chi(x)^{ay}\chi(1 + p^{\alpha-1}(p-1)\overline{x}t/f)^{ay} = \chi(x)^{ax}\zeta_p^{-(p-1)avt/f}$$

since $\chi^a = \psi^{av}$ has order dividing $\phi(q)/f$. Thus

$$\chi(y)^{ay}\zeta_q^{by} = \chi(x)^{ax}\zeta_p^{-(p-1)avt/f}\zeta_q^{bx+p^{\alpha-1}(p-1)bt/f} = \chi(x)^{ax}\zeta_q^{bx}\zeta_p^{-(p-1)(av-b)t/f} = \chi(x)^{ax}\zeta_q^{bx}.$$

I am ready to state the main result.

THEOREM 3. *Let $\chi = \psi^v$ be a primitive character modulo $q = p^\alpha$ where $f = \gcd(av, p-1)$ and $p\nmid b$ with $av \equiv b \pmod{p}$. Then*

$$\sum_{x=1,\,p\nmid x}^{\phi(q)/f} \chi(x)^{ax}\zeta_q^{bx} = \begin{cases} \frac{p-1}{f}p^{(\alpha-2)/2}\sum_{x\in H}\zeta_q^{bxg^{p-1}(1+pka\bar{b}vt)}, \\ \left(\frac{-2}{p}\right)\frac{p-1}{f}p^{(\alpha-3)/2}i^*\sqrt{p}\sum_{x\in H}\left(\frac{bx}{p}\right)\zeta_q^{bxg^{(p-1)t}(1+pka\bar{b}vt)} \end{cases}$$

*according as $\alpha \ge 2$ is even or odd, where $t$ satisfies $pkavt \equiv av - b \pmod{p^{s'}}$ for $0 \le t < p^{s'-1}$. Here $H$ is the group of $f$-roots of unity modulo $q$.*

*Proof.* From Lemma 3,

$$\sum_{x=1,\,p\nmid x}^{\phi(q)/f} \chi(x)^{ax}\zeta_q^{bx} = \frac{1}{p}\sum_{x=1,\,p\nmid x}^{q(p-1)/f}\chi(x)^{ax}\zeta_q^{bx} = \frac{1}{p}\sum_{j=0}^{(p-1)/f-1}\sum_{i=0}^{\phi(q)-1}\chi(g^i)^{av(g^i+jq)}\zeta_q^{bg^i},$$

where each $x$ is uniquely written as $x = g^i + jq \pmod{q(p-1)}$ for $0 \le i < \phi(q)$ and $0 \le j < (p-1)/f$. But the rightmost sum above equals

$$\frac{1}{p}\sum_{j=0}^{(p-1)/f-1}\sum_{i=0}^{\phi(q)-1}\zeta_{q(p-1)}^{apkvi(g^i+jq)+b(p-1)g^i} = \frac{1}{p}\sum_{i=0}^{\phi(q)-1}\zeta_{q(p-1)}^{b(a\bar{b}pkvi+p-1)g^i}\sum_{j=0}^{(p-1)/f-1}\zeta_{p-1}^{apkvij}.$$

Since $f = \gcd(av, p-1)$,

$$\sum_{j=0}^{(p-1)/f-1}\zeta_{p-1}^{apkvij} = \begin{cases} (p-1)/f & \text{if } i \equiv 0 \pmod{(p-1)/f}, \\ 0 & \text{otherwise,} \end{cases}$$

so the last summation becomes

$$\frac{1}{p}\frac{p-1}{f}\sum_{i=0}^{fp^{\alpha-1}-1}\zeta_{q(p-1)}^{b(a\bar{b}kvp(p-1)i/f+p-1)g^{(p-1)i/f}}. \tag{28}$$

Noting that each integer $i$ with $0 \le i < fp^{\alpha-1}$ can be uniquely expressed modulo $fp^{\alpha-1}$ as

$$i = wp^{\alpha-1} + jf \quad \text{for } 0 \le w < f,\ 0 \le j < p^{\alpha-1},$$

the sum (28) may be written as

$$\frac{p-1}{pf}\sum_{w=0}^{f-1}\sum_{j=0}^{p^{\alpha-1}-1}\zeta_{q(p-1)}^{b(a\bar{b}kvp(w(p-1)p^{\alpha-1}/f+j(p-1))+p-1)g^{\phi(q)w/f}g^{(p-1)j}} = \frac{p-1}{pf}\sum_{w=0}^{f-1}\sum_{j=0}^{p^{\alpha-1}-1}\zeta_q^{g^{(p-1)j}(1+pka\bar{b}vj)bg^{\phi(q)w/f}}$$

or

$$\frac{p-1}{pf}\sum_{x\in H}\sum_{j=0}^{p^{\alpha-1}-1}\zeta_q^{bxg^{(p-1)j}(1+pka\bar{b}vj)}.$$

Here I use the facts that $f \mid av$ and $g^{\phi(q)/f}$ generates the group $H$ of $f$-roots of unity modulo $q$. The result stated in the theorem now follows from Proposition 3.

For the special case when $av \equiv b \pmod{p^{s'}}$ one finds from Corollary 1 that

Corollary 10. *With the same hypotheses as in Theorem* 3, *if* $av \equiv b \pmod{p^{s'}}$ *then*

$$\sum_{x=1,\, p\nmid x}^{\phi(q)/f}\chi(x)^{ax}\zeta_q^{bx} = \begin{cases} \frac{p-1}{f}p^{(\alpha-2)/2}\sum_{x\in H}\zeta_q^{bx}, \\ \left(\frac{-2}{p}\right)\frac{p-1}{f}p^{(\alpha-3)/2}i^*\sqrt{p}\sum_{x\in H}\left(\frac{bx}{p}\right)\zeta_q^{bx} \end{cases}$$

*according as* $\alpha \geq 2$ *is even or odd*, *independent of the choice of generating character* $\psi$ *satisfying* (6).

Comparing the results of Theorems 1 and 3 one also notes

Corollary 11. *With the same hypotheses as in Theorem* 3, *if* $av \equiv b \pmod{p}$ *and* $a \equiv 0 \pmod{p-1}$ *then*

$$\sum_{x=1,\, p\nmid x}^{p^{\alpha-1}}\chi(x)^{ax}\zeta_q^{bx} = \frac{1}{p}\,S(a,b,\chi,q).$$

In closing, I remark that to determine the incomplete sum (5) when $av \not\equiv b \pmod{p}$ remains an open question.

## References


[1] B. C. Berndt, R. J. Evans and K. S. Williams, *Gauss and Jacobi Sums*, Wiley-Interscience, New York, 1998.

[2] Z. I. Borevich and I. R. Shafarevich, *Number Theory*, Academic Press, New York, 1966.

[3] T. Cochrane, *Exponential sums modulo prime powers*, Acta Arith. 101 (2002), 131–149.

[4] T. Cochrane and Z. Y. Zheng, *A survey on pure and mixed exponential sums modulo prime powers*, in: Number Theory for the Millennium, I, M. A. Bennett *et al.* (eds.), A K Peters, Natick, MA, 2002, 273–300.
[5] —, —, *Exponential sums with rational function entries*, Acta Arith. 95 (2000), 67–95.
[6] R. J. Evans, *Twisted hyper-Kloosterman sums over finite rings of integers*, in: Number Theory for the Millennium, I, M. A. Bennett *et al.* (eds.), A K Peters, Natick, MA, 2002, 429–448.
[7] S. Gurak, *Minimal polynomials for Gauss periods with* $f = 2$, Acta Arith. 121 (2006), 233–257.
[8] —, *On the minimal polynomial of Gauss periods for prime powers*, Math. Comp. 75 (2006), 2021–2035.
[9] —, *Explicit values of multi-dimensional Kloosterman sums for prime powers*, to appear.
[10] J. L. Mauclaire, *Sommes de Gauss modulo* $p^\alpha$, *I*, Proc. Japan Acad. Ser. A Math. Sci. 59 (1983), 109–112.
[11] —, *Sommes de Gauss modulo* $p^\alpha$, *II*, ibid., 161–163.
[12] H. Salié, *Über die Kloostermanschen Summen* $S(u, v; q)$, Math. Z. 34 (1932), 91–109.

Department of Mathematics
University of San Diego
San Diego, CA 92110, U.S.A.
E-mail: gurak@sandiego.edu

*Received on 19.5.2006*
*and in revised form on 28.9.2006* (5202)