*Functiones et Approximatio*
*51.2 (2014), 285–301*
*doi: 10.7169/facm/2014.51.2.4*

# TWISTED MONOMIAL GAUSS SUMS MODULO PRIME POWERS

Vincent Pigno, Christopher Pinner

**Abstract:** We show that twisted monomial Gauss sums modulo prime powers can be evaluated explicitly once the power is sufficiently large.

**Keywords:** exponential sums, Gauss sums.

## 1. Introduction

For a multiplicative character $\chi$ mod $q$ and $f(x) \in \mathbb{Z}[x]$ we define the twisted Gauss sum

$$S(\chi, f(x), q) := \sum_{x=1}^{q} \chi(x) e_q(f(x))$$

where $e_q(x) = e^{2\pi i x/q}$. We are concerned here with evaluating these sums when $f(x) = nx^k$ is a monomial and the modulus is a prime power $q = p^m$ with $m \geqslant 2$. If $(q_1, q_2) = 1$ and we write the mod $q_1q_2$ character as a product of mod $q_i$ characters $\chi_i$, then straightforwardly

$$S(\chi_1\chi_2, nx^k, q_1q_2) = \chi_1(q_2)\chi_2(q_1)S(\chi_1, nq_2^{k-1}x^k, q_1)S(\chi_2, nq_1^{k-1}x^k, q_2). \quad (1)$$

Hence it is usually enough to consider the case of a prime power modulus $S(\chi, nx^k, p^m)$. Obtaining satisfactory bounds, other than the Weil bound [17], remains a difficult problem when $m = 1$ (see for example Heath-Brown and Konyagin [9]). For higher powers though, methods of Cochrane and Zheng [3] can often be used to reduce the modulus of an exponential sum and sometimes evaluate the sum exactly.

When the modulus $q$ is squarefull, i.e. $p \mid q \Rightarrow p^2 \mid q$, and $(2nk, q) = 1$, Zhang and Liu [18] consider the fourth power mean value of $|S(\chi, nx^k, q)|$, averaged over

**2010 Mathematics Subject Classification:** primary: 11L05; secondary: 11L07, 11L03

the characters $\chi \bmod q$,

$$\sum_{\chi \bmod q} \left|S(\chi, nx^k, q)\right|^4 = q\phi^2(q) \prod_{p|q} (k, p-1)^2, \tag{2}$$

(their formula contains an additional factor when there are primes $p \mid q$ with $(k, p-1) = 1$ due to an apparent miscount in their Lemma 5). In the quadratic case, $\left|S(\chi, nx^2, q)\right|$, He and Zhang [7] obtain similar exact expressions for the sixth and eighth power means when $q$ is squarefull and coprime to $2n$, making the conjecture, subsequently proved by Liu and Yang [10], that

$$\sum_{\chi \bmod q} |S(\chi, nx^2, q)|^{2\ell} = 4^{(\ell-1)\omega(q)} q^{\ell-1} \phi^2(q), \qquad \omega(q) := \sum_{p|q} 1, \tag{3}$$

for any integer $\ell \geqslant 2$. Similarly Guo Xiaoyan and Wang Tingting [6] consider power means averaged over the parameter $n$ for quadratic and cubic sums, again $q$ squarefull with $(2n, q) = 1$ and $(6n, q) = 1$ respectively, showing that for any real $\ell \geqslant 0$,

$$\sum_{\substack{n=1 \\ (n,q)=1}}^{q} |S(\chi, nx^2, q)|^{2\ell} = 2^{(2\ell-1)\omega(q)} q^{\ell} \phi(q), \tag{4}$$

when $\chi$ is the square of a primitive character mod $q$ (and zero otherwise), and

$$\sum_{\substack{n=1 \\ (n,q)=1}}^{q} |S(\chi, nx^3, q)|^4 = 27^{\omega_1(q)} q^2 \phi(q), \qquad \omega_1(q) := \sum_{\substack{p|q \\ 3|p-1}} 1, \tag{5}$$

when $\chi$ is the cube of a primitive character mod $q$ (and zero otherwise). These average results all generalize to arbitrary monomials $nx^k$ and arbitrary real power means as we show in Corollary 1.1 below.

Actually, the methods in Cochrane and Zheng [3] can be used to evaluate the individual sums $S(\chi, nx^k, p^m)$ directly when $m \geqslant 2$, $(p, 2nk) = 1$, with no need to average. The approach of Cochrane and Zheng involves finding a set of non-zero critical points $\alpha$ satisfying a congruence, which in this case takes the simple form

$$rkx^k + c \equiv 0 \mod p, \tag{6}$$

(with the integers $r$ and $c$ defined in (17) below), and reducing the exponential sum to a sum of exponential sums, $S_\alpha$, over the $x \equiv \alpha \bmod p$ . When the critical points have multiplicity one the $S_\alpha$ can be evaluated explicitly. For example if $f(x) = x$ then as observed in Cochrane and Zheng [5, §9] the critical point congruence is simply $rx + c \equiv 0 \bmod p$. So for $p$ odd and $m \geqslant 2$, if $\chi$ is imprimitive there is no critical point and $S(\chi, x, p^m) = 0$, while if $\chi$ is primitive there is one critical point of multiplicity one and

$$S(\chi, x, p^m) = \chi(\alpha^*) e_{p^m}(\alpha^*) p^{m/2} \left(\frac{-2rc}{p^m}\right) \epsilon, \tag{7}$$

where $\left(\frac{x}{p^m}\right)$ denotes the Jacobi symbol,

$$\epsilon := \begin{cases} 1, & \text{if } p^m \equiv 1 \bmod 4, \\ i, & \text{if } p^m \equiv 3 \bmod 4, \end{cases} \tag{8}$$

and

$$R\alpha^* \equiv -c \bmod p^{[(m+1)/2]} \tag{9}$$

with $R$ the $p$-adic integer $R := p^{-1}\log(1+rp)$ (a small adjustment is needed in (9) in the case $p = m = 3$, see (20) below, and more generally in [3, Theorem 1.1(iii)] when $p = m - t = 3$). The same formula (7) occurs in Mauclaire [13] with $\alpha^*$ defined by $\chi(1+p^{m/2}) = e_{p^{m/2}}(-\alpha^*)$ when $m$ is even and $\chi(1+p^{(m-1)/2} + 2^{-1}p^{m-1}) = e_{p^{(m+1)/2}}(-\alpha^*)$ when $m$ is odd. Mauclaire also deals with the case $p = 2$ in [14]. A variation of (7) was obtained by Odoni [15] (see also Berndt, Evans and Williams [2, Theorems 1.6.2-1.6.4]).

Moreover (due to the straightforward relationship between the $\alpha$ satisfying (6)) for general $f(x) = nx^k$, $(2nk, p) = 1$, $m \geqslant 2$, the $\sum S_\alpha$ arising in Cochrane and Zheng's method will, with a little work, still simplify down to a single term of modulus $(k, p-1)p^{m/2}$. When $p \mid k$ though the critical points are multiple roots so the method is not directly applicable. However we show here that Cochrane and Zheng's method can be adjusted to deal with $p \mid k$. Additionally our approach reduces to finding a single solution of a certain *characteristic equation* (18) or (19), avoiding the need to sum as with the original $S_\alpha$.

Working mod $p^m$ we write

$$f(x) = nx^{\gamma p^t}, \qquad p \nmid \gamma n, \tag{10}$$

and define

$$d = (\gamma, p-1). \tag{11}$$

Analogous to the squarefull condition in [6], [7], [10] and [18] we shall assume that

$$m \geqslant t+2. \tag{12}$$

**Theorem 1.1.** *Let $p$ be an odd prime, $\chi$ be a character mod $p^m$ and suppose that* (10) *and* (12) *hold.*

*If $\chi$ is the $dp^t$-th power of a primitive character mod $p^m$ and an appropriate characteristic equation* (18) *or* (19) *has a solution then*

$$\left|S(\chi, nx^{\gamma p^t}, p^m)\right| = dp^\tau$$

*where*

$$\tau = \begin{cases} m-1, & \text{if } \ t+1 < m \leqslant 2t+2, \\ \frac{m}{2}+t, & \text{if } \ 2t+2 \leqslant m. \end{cases} \tag{13}$$

*Otherwise $S(\chi, nx^{\gamma p^t}, p^m) = 0$.*

Theorem 1.1 is an immediate consequence of Theorem 2.1 where we state an explicit formula for $S(\chi, nx^{\gamma p^t}, p^m)$. The corresponding result for $p = 2$ is given in (39). Averaging over the $n$ or $\chi$ we imediately obtain:

**Corollary 1.1.** *Under the same hypotheses of Theorem 1.1. For any real $b > 0$,*

$$\sum_{\chi \bmod p^m} |S(\chi, nx^{\gamma p^t}, p^m)|^b = (dp^\tau)^b \frac{\phi^2(p)}{d^2} p^{\max\{m-2t-2,0\}}, \tag{14}$$

*and when $\chi$ is a $dp^t$-th power of a primitive character mod $p^m$,*

$$\sum_{\substack{n=1 \\ (n,p)=1}}^{p^m} |S(\chi, nx^{\gamma p^t}, p^m)|^b = (dp^\tau)^b \frac{\phi(p)}{d} p^{\max\{m-t-1,\, t+1\}}. \tag{15}$$

The corresponding results for composite moduli (including (2–5)) then follow immediately from the multiplicativity (1). Since Theorem 1.1 shows that the $|S(\chi, nx^{\gamma p^t}, p^m)|$ can assume only one nonzero value, power means are somewhat artificial here, with (14) and (15) amounting only to a count on the number of non-zero cases (we include them for comparison with results in the literature and to emphasize that the restriction to certain integer power means is unnecessary).

The condition (12) is appropriate here. For $t \geqslant m$ the exponent reduces by Euler's Theorem and as shown in the proof of Theorem 2.1 (see (27)) when $m = t + 1$ the sum is zero unless $\chi$ is a mod $p$ character, in which case it reduces to a Heilbronn type mod $p$ sum

$$S(\chi, nx^{\gamma p^{m-1}}, p^m) = p^{m-1} \sum_{x=1}^{p-1} \chi(x) e_{p^m}(nx^{\gamma p^{m-1}}).$$

For $m = 2$ and $d = 1$ these are the classical Heilbronn sums, bounded using the Stepanov method by Heath-Brown [8] and Heath-Brown and Konyagin [9], extended by Puchta [16] and improved by Malykhin [11] to deal with $d = (\gamma, p-1) > 1$

$$\left| \sum_{x=1}^{p-1} e_{p^2}(nx^{\gamma p}) \right| \ll d^{1/2} p^{7/8}.$$

We note that their methods would allow the inclusion of a mod $p$ character $\chi$. Obtaining exact values seems unlikely for these types of sum. In [12] Malykhin considers the general case $m > 2$, for example obtaining

$$\left| \sum_{x=1}^{p-1} e_{p^m}\left(nx^{p^{m-1}}\right) \right| \leqslant C(m) p^{1-1/32 \cdot 5^{m-3}}.$$

We have assumed here that $p \nmid n$. If $p \mid n$ and $\chi$ is a primitive character mod $p^m$ then $S(\chi, nx^{\gamma p^t}, p^m) = 0$ as can be seen from the proof of Theorem 2.1 (if $p \mid n$ and $p \nmid c$ then the characteristic equation (24) or (29) will have no solution). If $p \mid n$ and $\chi$ is a mod $p^{m-1}$ character then plainly we can reduce to a mod $p^{m-1}$ sum.

## 2. Preliminaries

Suppose that $p$ is an odd prime and $a$ is a primitive root mod $p^l$ for all $l$. We define the integers $r(l)$, $p \nmid r(l)$, by

$$a^{\phi(p^l)} = 1 + r(l)p^l, \tag{16}$$

and the integers $r$ and $c$ by

$$r := r(1), \qquad \chi(a) = e\left(c/\phi(p^m)\right), \tag{17}$$

where $e(y) = e^{2\pi i y}$. Note that $\chi$ is a primitive character mod $p^m$ if and only if $p \nmid c$.

We first observe that $S(\chi, nx^{\gamma p^t}, p^m) = 0$ if $\chi$ is not a $\gamma p^t$th power of a character. An alternative proof of this result will occur during the proof of Theorem 2.1 below.

**Lemma 2.1.** *For any odd prime $p$, multiplicative character $\chi$ mod $p^m$ and integer $n$, the sum $S(\chi, nx^k, p^m) = 0$ unless $\chi = \chi_1^k$ for some mod $p^m$ character $\chi_1$.*

**Proof.** Taking $z = a^{\phi(p^m)/(k,\phi(p^m))}$ we have $z^k = 1$ and

$$S(\chi, nx^k, p^m) = \sum_{x=1}^{p^m} \chi(x) e_{p^m}(nx^k) = \sum_{x=1}^{p^m} \chi(zx) e_{p^m}(n(zx)^k) = \chi(z) S(\chi, nx^k, p^m).$$

Hence if $S(\chi, nx^k, p^m) \neq 0$ we must have $\chi(a)^{\phi(p^m)/(k,\phi(p^m))} = \chi(z) = 1$ and

$$\chi(a) = e\left(c'(k, \phi(p^m))/\phi(p^m)\right)$$

for some integer $c'$. So $\chi$ is the $(k, \phi(p^m))$th power of a character mod $p^m$. Solving the linear equation

$$kx \equiv c'(k, \phi(p^m)) \mod \phi(p^m)$$

for some integer $c_1$ we can equivalently write

$$\chi(a) = e\left(c_1 k/\phi(p^m)\right),$$

and $\chi = \chi_1^k$ where $\chi_1$ is the mod $p^m$ character with $\chi_1(a) = e\left(c_1/\phi(p^m)\right)$. ■

If $\chi$ is the $\gamma p^t$th power of a character $\chi_1$ and $c_1$ an integer such that

$$\chi_1(a) = e\left(c_1/\phi(p^m)\right)$$

then our final characteristic equation will take one of the two following forms (depending on the size of $t$ relative to $m$).

*Case I:* When $t + 1 < m \leqslant 2t + 2$

$$c_1 + r_1 n x^{\gamma p^t} \equiv 0 \mod p^{m-t-1}, \qquad r_1 := r(t+1). \tag{18}$$

*Case II:* When $2t+2<m$

$$c_1+r_2nx^{\gamma p^t}\equiv 0 \mod p^{t+s+1}, \qquad r_2:=r(t+s+1), \tag{19}$$

where

$$s:=\max\left\{0,\left\lceil\frac{m}{3}\right\rceil-t-1\right\}.$$

Expressions simplify slightly in Case II if we use the stronger congruence

$$c_1+r_3nx^{\gamma p^t}\equiv 0 \mod p^{\lceil\frac{m}{2}\rceil}, \qquad r_3:=r\left(\left\lceil\frac{m}{2}\right\rceil\right), \tag{20}$$

except for $p=3$, $m=3$, $t=0$ when we need $c_1+r_3nx^{\gamma}\equiv -3c_1r_2^2 \mod 9$.

Notice that, since $x^k$ and $x^{(k,\phi(p^m))}$ run through the same set of values mod $p^m$,

$$S(\chi_1^k,nx^k,p^m)=S(\chi_1^{(k,\phi(p^m))},nx^{(k,\phi(p^m))},p^m), \tag{21}$$

and so one can always reduce to a monomial $nx^{dp^t}$ with $d\mid p-1$, though we shall not assume this here.

**Theorem 2.1.** *For $p$ an odd prime, $t\in\mathbb{Z}$, $t\geqslant 0$, let*

$$f(x)=nx^{\gamma p^t}, \qquad p\nmid n\gamma.$$

*Case I: Suppose that $t+1<m\leqslant 2t+2$. If $\chi$ is a $dp^t$-th power of a primitive character and the characteristic equation* (18) *has a solution $\alpha$ then*

$$S(\chi,f(x),p^m)=dp^{m-1}\chi(\alpha)e_{p^m}(f(\alpha)).$$

*Otherwise, $S(\chi,f(x),p^m)=0$.*

*Case II: Suppose that $2t+2<m$. If $\chi$ is a $dp^t$-th power power of a primitive character and* (19) *has a solution then*

$$S(\chi,f(x),p^m)=dp^{\frac{m}{2}+t}\chi(\alpha)e_{p^m}(f(\alpha))\left(\frac{-2rc_1}{p^m}\right)\epsilon, \tag{22}$$

*where $\alpha$ is a solution of* (20)*, and $r$ and $\epsilon$ are as in* (17) *and* (8)*. Otherwise $S(\chi,f(x),p^m)=0$.*

Note in Case II we can use a solution $\alpha$ to the weaker congruence (19) if we include in (22) an additional factor

$$e_{p^{m-2t-2s-2}}(-2^{-2}\beta_1^{-1}\beta_2^2) \tag{23}$$

where, writing $c_1+r_2n\alpha^{\gamma p^t}=\lambda_1p^{t+s+1}$, $\beta_1:=-2^{-1}r_2c_1$, $\beta_2:=\lambda_1-\beta_1$. Here and throughout $x^{-1}$ denotes the multiplicative inverse of $x$ mod $p^m$.

## 3. Proof of Theorem 2.1

We start by rewriting the sum in terms of our primitive root $a$

$$S(\chi, nx^{\gamma p^t}, p^m) = \sum_{\substack{x=1 \\ p\nmid x}}^{p^m} \chi(x) e_{p^m}(nx^{\gamma p^t}) = \sum_{k=1}^{\phi(p^m)} \chi(a^k) e_{p^m}(na^{k\gamma p^t}).$$

We set $\gamma = d\gamma'$, where recall $d = (\gamma, p-1)$, and let $c$ be an integer such that

$$\chi(a) = e\left(\frac{c}{\phi(p^m)}\right) = e\left(\frac{c}{p^{m-1}(p-1)}\right).$$

*Case I:* Suppose that $t+1 < m \leqslant 2t+2$.

We let $u = 1, ..., dp^{m-1}$ and let $v$ run through an interval $I$ of $\frac{p-1}{d}$ consecutive integers so that $k = u\frac{p-1}{d} + v$ sums over $\phi(p^m)$ consecutive integers and

$$\begin{aligned}\sum_{k=1}^{\phi(p^m)} \chi(a^k) e_{p^m}(na^{k\gamma p^t}) &= \sum_{v\in I} \sum_{u=1}^{dp^{m-1}} \chi(a^{u\frac{p-1}{d}+v}) e_{p^m}(na^{(u\frac{p-1}{d}+v)\gamma p^t}) \\ &= \sum_{v\in I} \chi(a^v) e_{p^m}(na^{\gamma p^t v}) \\ &\quad \times \sum_{u=1}^{dp^{m-1}} e\left(\frac{cu}{dp^{m-1}}\right) e_{p^m}\left(na^{\gamma p^t v}\left(a^{p^t(p-1)\gamma' u} - 1\right)\right).\end{aligned}$$

Since $2(t+1) \geqslant m$ the binomial expansion gives

$$a^{p^t(p-1)\gamma' u} - 1 = (1 + r_1 p^{t+1})^{\gamma' u} - 1 \equiv \gamma' u r_1 p^{t+1} \bmod p^m,$$

and the inner sum becomes

$$\sum_{u=1}^{dp^{m-1}} e\left(\frac{u(c + r_1 p^t \gamma n a^{\gamma p^t v})}{dp^{m-1}}\right) = dp^{m-1}$$

if $v$ satisfies

$$c + r_1 p^t \gamma n a^{\gamma p^t v} \equiv 0 \bmod dp^{m-1}, \tag{24}$$

and zero otherwise. So we must examine when (24) has solutions.

Since $d \mid r_1 p^t \gamma n a^{\gamma p^t v}$, in order to have a solution we must have $d \mid c$ . Similarly, since $p \nmid r_1 \gamma n$ and $t < m-1$, we must have that $p^t || c$. So $\chi$ is a $dp^t$th power of a primitive character. Letting $c = c' p^t d$ and $\gamma = d\gamma'$ reduces our congruence to

$$c' + r_1 \gamma' n a^{\gamma p^t v} \equiv 0 \bmod p^{m-t-1}. \tag{25}$$

Hence (25) has no solution and $S(\chi, nx^{\gamma p^t}, p^m) = 0$ if there is no solution to the characteristic equation

$$c' + r_1 \gamma' n x^{\gamma p^t} \equiv 0 \bmod p^{m-t-1}. \tag{26}$$

If this equation has a solution $\alpha = a^{v_0}$ we take $I$ to be an interval containing $v_0$. Solutions $v$ to (25) must then satisfy $a^{\gamma p^t v} \equiv a^{\gamma p^t v_0} \bmod p^{m-t-1}$, that is $\gamma p^t v \equiv \gamma p^t v_0 \bmod p^{m-t-2}(p-1)$. Since $t \geqslant m-t-2$ this reduces to

$$v \equiv v_0 \bmod (p-1)/d,$$

and we have exactly the one solution $v = v_0$ in our range for $v$.

Hence

$$S(\chi, nx^{\gamma p^t}, p^m) = dp^{m-1}\chi(\alpha)e_{p^m}(f(\alpha)).$$

Writing $c = \gamma p^t c_1 \bmod \phi(p^m)$ we have $c' \equiv c_1\gamma' \bmod p^{m-t-1}$ and so the characteristic equation (26) can be written equivalently in the form (18).

Note: If $m = t+1$ the same analysis gives $p^{m-1} \mid c$ and $\chi$ is a mod $p$ character, and the sum reduces to

$$S(\chi, nx^{p^{m-1}\gamma}, p^m) = p^{m-1}\sum_{x=1}^{p}\chi(x)e_{p^m}(nx^{p^{m-1}\gamma}). \tag{27}$$

*Case II:* Suppose that $2t+2 < m$.

We now let $s = \max\{\lceil \frac{m}{3} \rceil - t - 1, 0\}$, $u = 1, ..., dp^{m-s-1}$ and let $v$ run through an interval $I$ of $p^s(\frac{p-1}{d})$ consecutive integers where $d := (\gamma, p-1)$ as before. Letting $k = up^s(\frac{p-1}{d}) + v$ we are still summing over $\phi(p^m)$ consecutive terms and

$$\begin{aligned}\sum_{k=1}^{\phi(p^m)}\chi(a^k)e_{p^m}(na^{k\gamma p^t}) &= \sum_{v\in I}\sum_{u=1}^{dp^{m-s-1}}\chi(a^{up^s(\frac{p-1}{d})+v})e_{p^m}(na^{(up^s(\frac{p-1}{d})+v)\gamma p^t}) \\ &= \sum_{v\in I}\chi(a^v)e_{p^m}(f(a^v))\sum_{u=1}^{dp^{m-s-1}} e\left(\frac{cu}{dp^{m-1-s}}\right) \\ &\quad \times e_{p^m}\left(na^{\gamma p^t v}\left(a^{p^{t+s}(p-1)\gamma' u}-1\right)\right).\end{aligned} \tag{28}$$

Expanding binomially, observing that $3(t+s+1) \geqslant m$, we obtain

$$\begin{aligned}a^{p^{t+s}(p-1)\gamma' u} - 1 &= \left(1 + r_2 p^{t+s+1}\right)^{\gamma' u} - 1 \\ &\equiv u\gamma' r_2 p^{t+s+1} + 2^{-1}u\gamma'(u\gamma'-1)r_2^2 p^{2t+2s+2} \bmod p^m,\end{aligned}$$

and the inner sum becomes

$$\sum_{u=1}^{dp^{m-s-1}} e\left(\frac{u\left(c + r_2\gamma n a^{\gamma p^t v}p^t + 2^{-1}\gamma r_2^2(u\gamma'-1)na^{\gamma p^t v}p^{2t+s+1}\right)}{dp^{m-s-1}}\right).$$

We now let $w = 1, ..., dp^{2t+s+1}$ and $y = 1, ..., p^{m-2t-2s-2}$, noting that $m-2t-2s-2 \geqslant 0$ with equality only when $m = 4$, $t = 0$. Hence if $u = wp^{m-2t-2s-2} + y$

we again sum over $dp^{m-s-1}$ consecutive integers and we can split the $u$ sum as a product $S_1(v)S_2(v)$ of a $y$ sum and a $w$ sum, where

$$S_1(v) = \sum_{y=1}^{p^{m-2t-2s-2}} e\left(\frac{y\left(c + r_2\gamma n a^{\gamma p^t v} p^t + 2^{-1}\gamma r_2^2(y\gamma' - 1)n a^{\gamma p^t v} p^{2t+s+1}\right)}{dp^{m-s-1}}\right),$$

and

$$S_2(v) = \sum_{w=1}^{dp^{2t+s+1}} e\left(\frac{w\left(c + r_2\gamma n a^{\gamma p^t v} p^t\right)}{dp^{2t+s+1}}\right).$$

Now $S_2(v) = dp^{2t+s+1}$ if

$$c + \gamma r_2 n a^{p^t \gamma v} p^t \equiv 0 \bmod dp^{2t+s+1}, \tag{29}$$

and $S_2(v) = 0$ otherwise. So again we must examine when (29) has solutions. Right away we see that in order to have a solution $p^t || c$ and $d \mid c$, so our congruence reduces to

$$c' + \gamma' r_2 n a^{p^t \gamma v} \equiv 0 \bmod p^{t+s+1} \tag{30}$$

where $c = c' dp^t$, $p \nmid c'$ and $\chi$ is a $dp^t$th power of a primitive character. Thus if the characteristic equation

$$c' + \gamma' r_2 n x^{\gamma p^t} \equiv 0 \bmod p^{t+s+1} \tag{31}$$

has no solution we have $S(\chi, nx^{\gamma p^t}, p^m) = 0$. If it has a solution $\alpha = a^{v_0}$ we again choose $I$ to be an interval containing $v_0$. Hence if $v$ is a solution to (30) then $a^{\gamma p^t v} \equiv a^{\gamma p^t v_0} \bmod p^{t+s+1}$, that is $\gamma p^t v \equiv \gamma p^t v_0 \bmod p^{t+s}(p-1)$ reducing to

$$v \equiv v_0 \bmod p^s(p-1)/d.$$

So we have only the solution $v = v_0$ in $I$ and so by (28)

$$\begin{aligned} S(\chi, nx^{\gamma p^t}, p^m) &= \chi(a^{v_0}) e_{p^m}(f(a^{v_0})) S_1(v_0) S_2(v_0) \\ &= dp^{2t+s+1} \chi(\alpha) e_{p^m}(f(\alpha)) S_1(v_0). \end{aligned} \tag{32}$$

When $m = 4$, $t = 0$, plainly $S_1(v_0) = 1$. Otherwise writing

$$c' + \gamma' r_2 n a^{p^t \gamma v_0} = \lambda p^{t+s+1}, \qquad \delta_1 := -2^{-1} r_2 \gamma' c', \qquad \delta_2 := \lambda + 2^{-1} r_2 c',$$

observing that $3t + 2s + 2 \geqslant m - s - 1$ and that $y_1 = y + 2^{-1}\delta_1^{-1}\delta_2$ runs through a complete set of residues mod $p^{m-2t-2s-2}$ as $y$ does, we can rewrite $S_1(v_0)$ in terms of a classical, readily evaluated (see for example Apostol [1, §9.10 and Exercise 8.16]

or Berndt, Evans and Williams [2, Theorem 1.5.2]), quadratic Gauss sum:

$$\begin{aligned} S_1(v_0) &= \sum_{y=1}^{p^{m-2t-2s-2}} e\left(\frac{y\left(\lambda - 2^{-1}r_2(y\gamma'-1)c'\right)}{p^{m-2t-2s-2}}\right) \\ &= \sum_{y=1}^{p^{m-2t-2s-2}} e\left(\frac{\delta_1 y^2 + \delta_2 y}{p^{m-2t-2s-2}}\right) \\ &= e\left(-\frac{2^{-2}\delta_1^{-1}\delta_2^2}{p^{m-2t-2s-2}}\right) \sum_{y_1=1}^{p^{m-2t-2s-2}} e\left(\frac{\delta_1 y_1^2}{p^{m-2t-2s-2}}\right) \\ &= e\left(-\frac{2^{-2}\delta_1^{-1}\delta_2^2}{p^{m-2t-2s-2}}\right)\left(\frac{\delta_1}{p^m}\right) p^{\frac{m}{2}-t-s-1}\epsilon, \end{aligned}$$

with $\epsilon$ as given in (8).

Thus by (32)

$$S(\chi, f(x), p^m) = dp^{\frac{m}{2}+t}\chi(\alpha)e_{p^m}(f(\alpha))e_{p^{m-2t-2s-2}}(-2^{-2}\delta_1^{-1}\delta_2^2)\left(\frac{\delta_1}{p^m}\right)\epsilon \qquad (33)$$

if $\chi$ is a $dp^t$th power of a primitive character and $c'+\gamma' r_2 n x^{p^t\gamma} \equiv 0 \bmod p^{t+s+1}$ has a solution $\alpha$, and $S(\chi, f(x), p^m) = 0$ otherwise. Replacing $c' \equiv c_1\gamma' \bmod p^{m-t-1}$ we have $\lambda \equiv \lambda_1\gamma'$, $\delta_1 \equiv \beta_1{\gamma'}^2$, $\delta_2 \equiv \gamma'\beta_2 \bmod p^{m-t-1}$, with $\left(\frac{\delta_1}{p}\right) = \left(\frac{\beta_1}{p}\right) = \left(\frac{-2rc_1}{p}\right)$. Thus we obtain (22) with the additional factor (23). It remains to show that if we use a solution $\alpha$ to (19) satisfying the stronger congruence (20) then this additional factor is 1.

Plainly we can assume that $2(s+t+1) < m \leqslant 3(s+t+1)$ and $\lceil \frac{m}{2} \rceil \leqslant 2(s+t+1)$ with equality only when $s = t = 0$ and $m = 3$. We first note that

$$r_3 \equiv r_2 - 2^{-1}r_2^2 p^{s+t+1} + 3^{-1}r_2^3 p^{2(s+t+1)} \bmod p^{\lceil \frac{m}{2} \rceil},$$

where the last term vanishes unless $p = 3$, $m = 3$ and $t = 0$. To see this observe that

$$\begin{aligned} 1 + r_3 p^{\lceil \frac{m}{2} \rceil} &= \left(1 + r_2 p^{s+t+1}\right)^{p^{\lceil \frac{m}{2} \rceil - s - t - 1}} \\ &\equiv 1 + r_2 p^{\lceil \frac{m}{2} \rceil} + \frac{1}{2}r_2^2 p^{\lceil \frac{m}{2} \rceil + s + t + 1}\left(p^{\lceil \frac{m}{2} \rceil - s - t - 1} - 1\right) \\ &\quad + \frac{1}{6}r_2^3 p^{\lceil \frac{m}{2} \rceil + 2(s+t+1)}\left(p^{\lceil \frac{m}{2} \rceil - s - t - 1} - 1\right) \\ &\quad \times \left(p^{\lceil \frac{m}{2} \rceil - s - t - 1} - 2\right) \bmod p^{4(s+t+1)} \\ &\equiv 1 + p^{\lceil \frac{m}{2} \rceil}\left(r_2 - 2^{-1}r_2^2 p^{s+t+1} + 3^{-1}r_2^3 p^{2(s+t+1)}\right) \bmod p^{2\lceil \frac{m}{2} \rceil}. \end{aligned}$$

In particular $r_3 \equiv r_2 \bmod p^{s+t+1}$. Hence if $\alpha$ is a solution to (19), which also satisfies (20),

$$c_1 + r_2 n\alpha^{\gamma p^t} = \lambda_1 p^{s+t+1}, \qquad c_1 + r_3 n\alpha^{\gamma p^t} \equiv -c_1 3^{-1} r_2^2 p^{2(s+t+1)} \bmod p^{\lceil \frac{m}{2} \rceil},$$

then

$$c_1(r_3 - r_2) \equiv p^{s+t+1} \left( r_2\lambda_1 + c_1 3^{-1} r_2^3 p^{s+t+1} \right) \bmod p^{\lceil \frac{m}{2} \rceil},$$

and

$$-2^{-1} c_1 r_2 \equiv \lambda_1 \bmod p^{\lceil \frac{m}{2} \rceil - s - t - 1}.$$

Hence $\beta_2 \equiv 0 \bmod p^{\lceil \frac{m}{2} \rceil - s - t - 1}$ and $e_{p^{m-2t-2s-2}} \left( -2^{-2} \beta_1^{-1} \beta_2^2 \right) = 1$.

Finally we need to verify that a solution $a^{v_0}$ to (19) guarantees a solution $a^v$ of (20). Since $r_3 \equiv r_2 \bmod p^{s+t+1}$,

$$c_1 + r_3 n a^{v_0 \gamma p^t} = \lambda p^{s+t+1}$$

for some integer $\lambda$. Taking $v = v_0 + h\phi\left(p^{s+1}\right)$ we have

$$\begin{aligned} c_1 + r_3 n a^{v\gamma p^t} &= c_1 + r_3 n a^{v_0 \gamma p^t} a^{h\gamma\phi\left(p^{s+t+1}\right)} \\ &= \lambda p^{s+t+1} + r_3 n a^{v_0 \gamma p^t} \left( (1 + r_2 p^{s+t+1})^{\gamma h} - 1 \right) \\ &\equiv p^{s+t+1} \left( \lambda + r_3 n a^{v_0 \gamma p^t} \gamma r_2 h \right) \bmod p^{2(s+t+1)} \end{aligned}$$

and choosing $h$ with $\lambda + r_2^2 n a^{v_0 \gamma p^t} \gamma h \equiv -c_1 3^{-1} r_2^2 p^{s+t+1} \bmod p^{\lceil \frac{m}{2} \rceil - s - t - 1}$ gives the required solution. ∎

## 4. Proof of Corollary 1.1

From Theorem 2.1 we know that if $S(\chi, nx^{\gamma p^t}, p^m)$ is non zero then $\chi$ must be a $dp^t$th power of a primitive character mod $p^m$, and there must be a solution to a characteristic equation (26) or (31),

$$c' + r'\gamma' n x^{\gamma p^t} \equiv 0 \mod p^\kappa, \tag{34}$$

where $c = c' dp^t < \phi(p^m)$, $(nc', p) = 1$, and $r'$ and $\kappa$ depend on the range of $t$. If such is the case then $|S(\chi, nx^{\gamma p^t}, p^m)| = dp^\tau$. Thus to prove Corollary 1.1 we simply count the $\chi$ (i.e. count the $c'$) or $n$ that give us solutions. Writing in terms of our primitive root $x = a^v$, $-r'\gamma' n = a^{v_o}$, $c' = a^{v_1}$, (34) becomes,

$$(a^v)^{\gamma p^t} \equiv a^{v_1 - v_0} \mod p^\kappa,$$

which is equivalent to

$$\gamma p^t v \equiv v_1 - v_0 \mod \phi(p^\kappa).$$

This linear congruence in $v$ has a solution when

$$(\gamma p^t, \phi(p^\kappa)) = d(p^t, p^{\kappa-1}) = dp^{\min\{m-t-2,t\}}$$

divides $v_1 - v_0$. So we have $\frac{\phi(p^\kappa)}{dp^{\min\{m-t-2,t\}}}$ values of $c'$ mod $p^\kappa$ (or likewise values of $n$ mod $p^\kappa$) that yield solutions.

Note that $c'$ ranges from 1 to $\frac{\phi(p^m)}{dp^t} = p^\kappa \frac{p^{m-\kappa-t-1}(p-1)}{d}$, giving

$$\frac{\phi(p^\kappa)}{dp^{\min\{m-t-2,t\}}} \left( \frac{p^{m-\kappa-t-1}(p-1)}{d} \right) = \frac{\phi^2(p)}{d^2} p^{\max\{m-2t-2,0\}}$$

$c'$s that will allow a solution to our characteristic equation, and (14) is clear.

Similarly $n$ ranges over the terms relatively prime to $p$ from 1 to $p^m = p^\kappa(p^{m-\kappa})$,

$$\frac{\phi(p^\kappa)}{dp^{\min\{m-t-2,t\}}} p^{m-\kappa} = \frac{\phi(p)}{d} p^{\max\{m-t-1,t+1\}},$$

giving (15). ■

## 5. When $p = 2$, $m \geqslant 6$

We now examine the case when $p = 2$ and $m \geqslant 6$, giving sums of the form

$$S(\chi, nx^{\gamma 2^t}, 2^m) = \sum_{x=1}^{2^m} \chi(x) e_{2^m}(nx^{\gamma 2^t})$$

where $\chi$ is a character mod $2^m$, $n$ and $\gamma$ are odd, and $t \geqslant 0$. Since $x^{2^{m-2}} \equiv 1$ mod $2^m$ for any odd $x$ we shall assume that

$$t < m - 2.$$

When dealing with these sums the methods are nearly the same except that we need two generators, $a$ and $-1$, to generate all of $\mathbb{Z}_{2^m}^*$. Even so, this case is actually simpler computation-wise. As for odd $p$ we can also immediately say that $S(\chi, nx^k, 2^m) = 0$ unless $\chi = \chi_1^k$ for some character $\chi_1$ mod $2^m$. The proof of this is almost the same the proof of Lemma 2.1 (we get the same relation for $\chi(a)$ and, when $m > 2$ and the second generator $-1$ is needed, taking $z = -1$ in the same argument gives $\chi(-1) = 1$ if $k$ is even).

Here we write

$$\chi(a) = e\left(\frac{c}{2^{m-2}}\right)$$

and define the odd integer $r$ and when $t \geqslant 1$ the odd integer $r_1$ by

$$a^{2^{\lceil \frac{m}{2} \rceil - 2}} = 1 + r2^{\lceil \frac{m}{2} \rceil}, \qquad a^{2^t} = 1 + r_1 2^{t+2}. \tag{35}$$

We will have $S(\chi, nx^{2^t\gamma}, 2^m) = 0$ unless $c = 2^t c'$ with $c'$ odd, and our characteristic equation will take the form

$$c' + nr\gamma x^{2^t\gamma} \equiv 0 \bmod 2^{\lfloor \frac{m}{2} \rfloor}. \tag{36}$$

We first evaluate the sums

$$S(n) := \sum_{k=1}^{2^{m-2}} \chi(a^k) e_{2^m}(na^{k\gamma 2^t}).$$

**Lemma 5.1.** *Suppose that $c = 2^t c'$ with $c'$ odd. If $0 \leqslant t < \lceil \frac{m}{2} \rceil - 2$ and (36) has a solution $\alpha = a^{v_0}$ then*

$$S(n) = 2^{\lfloor \frac{m}{2} \rfloor + t} \chi(\alpha) e_{2^m}(n\alpha^{\gamma 2^t}) \psi,$$

*where*

$$\psi = \begin{cases} 1, & \text{if } m \text{ is even,} \\ 1 + (-1)^{(\frac{\gamma-1}{2}+\lambda)} i^{rc'}, & \text{if } m \text{ is odd,} \end{cases} \tag{37}$$

*with $\lambda$ defined by*

$$c' + nr\gamma\alpha^{\gamma 2^t} = \lambda 2^{\lfloor \frac{m}{2} \rfloor}. \tag{38}$$

*If $\lceil \frac{m}{2} \rceil - 2 \leqslant t < m - 2$ and $c' + nr_1\gamma \equiv 0 \bmod 2^{m-2-t}$ then*

$$S(n) = 2^{m-2} e\left(\frac{n}{2^m}\right).$$

*Otherwise $S(n) = 0$.*

**Proof.**

$$S(n) = \sum_{k=1}^{2^{m-2}} e\left(\frac{kc}{2^{m-2}}\right) e_{2^m}(na^{k\gamma 2^t}).$$

If $t + 2 \geqslant \lceil \frac{m}{2} \rceil$ then

$$na^{k\gamma 2^t} = n\left(1 + r_1 2^{t+2}\right)^{k\gamma} \equiv n\left(1 + r_1 k\gamma 2^{t+2}\right) \bmod 2^m,$$

and

$$S(n) = e\left(\frac{n}{2^m}\right) \sum_{k=1}^{2^{m-2}} e\left(\frac{k(c + nr_1\gamma 2^t)}{2^{m-2}}\right).$$

The sum is $2^{m-2}$ if $c + nr_1\gamma 2^t \equiv 0 \bmod 2^{m-2}$ (and zero otherwise). This only occurs when $c = 2^t c'$, $c'$ odd, with $c' + nr_1\gamma \equiv 0 \bmod 2^{m-t-2}$.

Suppose now that $t < \lceil \frac{m}{2} \rceil - 2$. We write $k = u2^{\lceil \frac{m}{2} \rceil - t - 2} + v$ where $v$ runs through an interval $I$ of length $2^{\lceil \frac{m}{2} \rceil - t - 2}$ and $u = 1, ..., 2^{\lfloor \frac{m}{2} \rfloor + t}$. Using (35) and

expanding binomially gives

$$\begin{aligned}
S(n) &= \sum_{v\in I}\sum_{u=1}^{2^{\lfloor \frac{m}{2}\rfloor+t}} e\left(\frac{(u2^{\lceil \frac{m}{2}\rceil-t-2}+v)c}{2^{m-2}}\right)e\left(\frac{na^{(u2^{\lceil \frac{m}{2}\rceil-t-2}+v)\gamma 2^t}}{2^m}\right)\\
&= \sum_{v\in I}\chi(a^v)e\left(\frac{na^{v\gamma 2^t}}{2^m}\right)\sum_{u=1}^{2^{\lfloor \frac{m}{2}\rfloor+t}} e\left(\frac{cu}{2^{\lfloor \frac{m}{2}\rfloor+t}}\right)e\left(\frac{na^{v\gamma 2^t}\left((1+r2^{\lceil \frac{m}{2}\rceil})^{u\gamma}-1\right)}{2^m}\right)\\
&= \sum_{v\in I}\chi(a^v)e\left(\frac{na^{v\gamma 2^t}}{2^m}\right)\sum_{u=1}^{2^{\lfloor \frac{m}{2}\rfloor+t}} e\left(\frac{u\left(c+nr\gamma 2^t a^{v\gamma 2^t}\right)}{2^{\lfloor \frac{m}{2}\rfloor+t}}\right).
\end{aligned}$$

So as in our previous cases we end up with a sum over a full set of residues and the inner sum is zero unless

$$c+nr\gamma 2^t a^{v\gamma 2^t}\equiv 0 \bmod 2^{\lfloor \frac{m}{2}\rfloor+t}.$$

In order to have a solution plainly $c=2^t c'$ for some odd $c'$, reducing our congruence to

$$c'+nr\gamma a^{v\gamma 2^t}\equiv 0 \bmod 2^{\lfloor \frac{m}{2}\rfloor}.$$

Thus $S(n)=0$ unless we have a solution $\alpha=a^{v_0}$ to our characteristic equation (36). We take $I$ to be the interval $\left[v_0, v_0+2^{\lceil \frac{m}{2}\rceil-t-2}\right]$. If $a^v$ is another solution then plainly

$$v\gamma 2^t\equiv v_0\gamma 2^t \bmod 2^{\lfloor \frac{m}{2}\rfloor-2},$$

and

$$v\equiv v_0 \bmod 2^{\lfloor \frac{m}{2}\rfloor-t-2}.$$

When $m$ is even $\lfloor \frac{m}{2}\rfloor=\lceil \frac{m}{2}\rceil$ and we only have the solution $v_0$ in our range for $v$, and

$$S(n)=2^{\frac{m}{2}+t}\chi(\alpha)e_{2^m}(n\alpha^{\gamma 2^t}).$$

When $m$ is odd we note that $2^{\lfloor \frac{m}{2}\rfloor-t-2}$ is half the range of $v$ and we have two solutions $\alpha=a^{v_0}$ and $a^{v_0+2^{\lfloor \frac{m}{2}\rfloor-t-2}}$. Plugging these in, using that $a^{2^{\left\lfloor \frac{m}{2}\right\rfloor-2}}=1+r'2^{\lfloor \frac{m}{2}\rfloor}$ for some odd $r'$ when $m\geqslant 6$, and expanding binomially, we get

$$\begin{aligned}
S(n) &= 2^{\lfloor \frac{m}{2}\rfloor+t}\left(\chi(a^{v_0})e_{2^m}(n(a^{v_0})^{\gamma 2^t})+\chi(a^{v_0+2^{\lfloor \frac{m}{2}\rfloor-t-2}})e_{2^m}(n(a^{v_0+2^{\lfloor \frac{m}{2}\rfloor-t-2}})^{\gamma 2^t}\right)\\
&= 2^{\lfloor \frac{m}{2}\rfloor+t}\chi(\alpha)e_{2^m}(n\alpha^{\gamma 2^t})\\
&\quad\times\left(1+\chi(a^{2^{\lfloor \frac{m}{2}\rfloor-t-2}})e_{2^m}(na^{v_0\gamma 2^t}\left((1+r'2^{\lfloor \frac{m}{2}\rfloor})^{\gamma}-1\right)\right)\\
&= 2^{\lfloor \frac{m}{2}\rfloor+t}\chi(\alpha)e_{2^m}(n\alpha^{\gamma 2^t})\\
&\quad\times\left(1+e\left(\frac{c'}{2^{\lceil \frac{m}{2}\rceil}}\right)e\left(\frac{nr'\gamma 2^{\lfloor \frac{m}{2}\rfloor}a^{v_0 2^t\gamma}+\frac{\gamma(\gamma-1)}{2}n(r')^2 2^{m-1}a^{v_0\gamma 2^t}}{2^m}\right)\right)\\
&= 2^{\lfloor \frac{m}{2}\rfloor+t}\chi(\alpha)e_{2^m}(n\alpha^{\gamma 2^t})\left(1+(-1)^{\frac{\gamma-1}{2}}e\left(\frac{c'+nr'\gamma a^{v_0\gamma 2^t}}{2^{\lceil \frac{m}{2}\rceil}}\right)\right).
\end{aligned}$$

We note that $a^{2^{\lceil \frac{m}{2} \rceil - 2}} = 1 + r2^{\lceil \frac{m}{2} \rceil} = (1 + r'2^{\lfloor \frac{m}{2} \rfloor})^2 = (a^{2^{\lfloor \frac{m}{2} \rfloor - 2}})^2$ giving us that

$$r' = r - (r')^2 2^{\lfloor \frac{m}{2} \rfloor - 1} \equiv r - 2^{\lfloor \frac{m}{2} \rfloor - 1} \bmod 2^{\lceil \frac{m}{2} \rceil}.$$

Plugging this in for $r'$ we get

$$e\left(\frac{c' + nr'\gamma a^{v_0\gamma 2^t}}{2^{\lceil \frac{m}{2} \rceil}}\right) = e\left(\frac{c' + nr\gamma a^{v_0\gamma 2^t}}{2^{\lceil \frac{m}{2} \rceil}}\right) e\left(\frac{-n\gamma a^{v_0\gamma 2^t}}{2^2}\right) = e\left(\frac{\lambda}{2}\right) e\left(\frac{c'r}{4}\right),$$

(using the characteristic equation and that $\left\lfloor \frac{m}{2} \right\rfloor \geqslant 2$) and the claimed result follows. ∎

**Theorem 5.1.** *Suppose that $\chi$ is a $2^t$th power of a primitive character mod $2^m$. If $0 \leqslant t < \left\lceil \frac{m}{2} \right\rceil - 2$ and (36) has a solution $\alpha$ then, with $\psi$ as in (37),*

$$S(\chi, nx^{\gamma 2^t}, 2^m) = 2^{\lfloor \frac{m}{2} \rfloor + t + \delta} \chi(\alpha) e_{2^m}(n\alpha^{\gamma 2^t})\psi, \qquad \delta = \begin{cases} 0, & \text{if } t = 0, \\ 1, & \text{if } t > 0. \end{cases}$$

*If $\left\lceil \frac{m}{2} \right\rceil - 2 \leqslant t < m - 2$ and $c' + nr_1\gamma \equiv 0 \bmod 2^{m-2-t}$ then*

$$S(\chi, nx^{\gamma 2^t}, 2^m) = 2^{m-1} e\left(\frac{n}{2^m}\right).$$

*Otherwise $S(\chi, nx^{\gamma 2^t}, 2^m) = 0$.*

Thus for $m \geqslant 6$ the non-zero values satisfy

$$\left|S(\chi, nx^{\gamma 2^t}, 2^m)\right| = 2^\tau, \qquad \tau = \begin{cases} \frac{m}{2}, & \text{if } t = 0, \\ \frac{m}{2} + t + 1, & \text{if } 0 < t < \left\lceil \frac{m}{2} \right\rceil - 2, \\ m - 1, & \text{if } \left\lceil \frac{m}{2} \right\rceil - 2 \leqslant t < m - 2. \end{cases} \tag{39}$$

**Proof.** We start by writing the sum in terms of the generators, $-1$ and $a$, of $\mathbb{Z}_{2^m}^*$

$$\begin{aligned} S(\chi, nx^{\gamma 2^t}, 2^m) &= \sum_{x=1}^{2^m} \chi(x) e_{2^m}(nx^{\gamma 2^t}) \\ &= \sum_{\omega=0}^{1} \sum_{k=1}^{2^{m-2}} \chi((-1)^\omega a^k) e_{2^m}(n((-1)^\omega a^k)^{\gamma 2^t}) \\ &= S(n) + \chi(-1) S((-1)^{2^t} n) \end{aligned}$$

If $t = 0$ then

$$S(\chi, nx^{\gamma 2^t}, 2^m) = S(n) + \chi(-1)S(-n).$$

By the lemma each $S(\pm n)$ is zero unless (36) has a solution $\alpha$. A solution will be either of the form $\alpha = a^{v_0}$ or $-a^{v_0}$ (since $m \geqslant 6$ we can not have solutions of both forms). By Lemma 5.1, in the first case $S(-n) = 0$ and

$$S(\chi, nx^{\gamma 2^t}, 2^m) = S(n) = 2^{\lfloor \frac{m}{2} \rfloor} \chi(\alpha) e_{2^m}(n\alpha^\gamma)\psi.$$

In the second case $S(n) = 0$ and

$$S(\chi, nx^{\gamma 2^t}, 2^m) = \chi(-1)S(-n) = \chi(-1)2^{\lfloor \frac{m}{2} \rfloor}\chi(-\alpha)e_{2^m}(-n(-\alpha)^\gamma)\psi.$$

If $t > 0$

$$S(\chi, nx^{\gamma 2^t}, 2^m) = S(n) + \chi(-1)S(n)$$

Thus if $\chi(-1) = -1$ our sum is zero. Otherwise

$$S(\chi, nx^{\gamma 2^t}, 2^m) = 2S(n)$$

and the result follows from the lemma. ■

## 6. Weil type bounds

From Theorem 1.2 one immediately obtains a Weil type bound for monomial sums

$$\left|S(\chi, nx^k, p^m)\right| \leqslant (k, \phi(p^m))p^{m/2} \tag{40}$$

when $p$ is odd, $p \nmid n$ and $\chi$ is a multiplicative character modulo $p^m$. When $p = 2$ an additional factor of 2 is needed. Cochrane and Zheng [4] have shown that such bounds do not hold for binomial sums. Multiplicativity then gives

$$\left|S(\chi, nx^k, q)\right| \leqslant \prod_{p^m || q} (k, \phi(p^m))q^{1/2} \leqslant (k, \phi(q))^{\omega(q)}q^{1/2}$$

for general odd modulus. The bound (40) can also be seen more directly. From Lemma 2.1 and observation (21) we can write any non-zero sum in the form $S(\chi_1^{k_1}, nx^{k_1}, p^m)$ where $k_1 = (k, \phi(p^m))$, and using a sum over the $k_1$ characters $\chi$ mod $p^m$ with $\chi_1^k = \chi_0$ to pick out the $k_1$-st powers,

$$\left|S(\chi_1^{k_1}, nx^{k_1}, p^m)\right| = \left|\sum_{\chi^{k_1} = \chi_0} \sum_{u=1}^{p^m} \chi\chi_1(u)e_{p^m}(nu)\right| \leqslant k_1 p^{m/2}.$$

## References


[1] T. Apostol, *Introduction to Analytic Number Theory*, Springer 1976.

[2] 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.

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

[4] T. Cochrane and Z. Zheng, *Bounds for certain exponential sums,* Asian J. Math. **4** (2000), no. 4, 757–774.

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

[6] X. Guo and T. Wang, *On the generalized $k$-th Gauss sums*, to appear Hacet. J. Math. Stat.

[7] Y. He and W. Zhang, *On the $2k$-th power mean value of the generalized quadratic Gauss sum*, Bull Korean Math. Soc. **48** (2011), 9–15.

[8] D.R. Heath-Brown, *An estimate for Heilbronn's exponential sum*, Analytic Number Theory: Proceedings of a conference in honor of Heini Halberstam, Birkhäuser, Boston, MA, (1996), 451–463.

[9] D.R. Heath-Brown and S. Konyagin, *New bounds for Gauss sums derived from kth powers, and for Heilbronn's exponential sum*, Quart. J. Math. **51** (2000), 221–235.

[10] F. Liu and Q.-H. Yang, *An identity on the $2m$-th power mean value of the generalized Gauss sums*, Bull. Korean Math. Soc. **49** (2012), no. 6, 1327–1334.

[11] Yu.V. Malykhin, *Bounds for exponential sums modulo $p^2$*, Journal of Mathematical Sciences **146**, No. 2, (2007), 5686-5696 [Translated from Fundamentalnaya i Prikladnaya Matematika **11**, No. 6, (2005), 81–94].

[12] Yu.V. Malykhin, *Estimates of trigonometric sums modulo $p^r$*, Mathematical Notes **80** (2006), No. 5, 748–752. [Translated from Matematicheskie Zametki **80** (2006), No. 5, 793–796].

[13] J.-L. Mauclaire, *Sommes de Gauss modulo $p^\alpha$. I*, Proc. Japan Acad. **59**, Ser A (1983), 109–112.

[14] J.-L. Mauclaire, *Sommes de Gauss modulo $p^\alpha$. II*, Proc. Japan Acad. **59**, Ser A (1983), 161–163.

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

[16] J-C. Puchta, *Remark on a paper of Yu on Heilbronn's exponential sum*, J. Number Theory **87** (2001), 239–241.

[17] A. Weil, *On some exponential sums*, Proc. Nat. Acad. Sci. U.S.A. **34** (1948), 203–210.

[18] W. Zhang and H. Liu, *On the general Gauss sums and their fourth power means*, Osaka J. Math. **42** (2005), 189–199.

**Address:** Vincent Pigno: Department of Mathematics and Statistics, California State University, Sacramento, Sacramento, CA 95819, USA;
Christopher Pinner: Department of Mathematics, Kansas State University, Manhattan, KS 66506, USA.

**E-mail:** vincent.pigno@csus.edu, pinner@math.ksu.edu

**Received:** 11 May 2013