JOURNAL
de Théorie des Nombres
de BORDEAUX

anciennement Séminaire de Théorie des Nombres de Bordeaux

Vincent PIGNO et Christopher PINNER

Binomial Character Sums Modulo Prime Powers

Tome 28, nº 1 (2016), p. 39-53.

<http://jtnb.cedram.org/item?id=JTNB_2016__28_1_39_0>

Journal de Théorie des Nombres
de Bordeaux **28** (2016), 39–53

Binomial Character Sums Modulo Prime Powers

par Vincent PIGNO et Christopher PINNER

Résumé. On montre que les sommes binomiales et liées de caractères multiplicatifs

$$\sum_{\substack{x=1\\(x,p)=1}}^{p^m} \chi(x^l(Ax^k+B)^w), \quad \sum_{x=1}^{p^m} \chi_1(x)\chi_2(Ax^k+B),$$

ont une évaluation simple pour m suffisamment grand (pour $m \geq 2$ si $p \nmid ABk$).

Abstract. We show that the binomial and related multiplicative character sums

$$\sum_{\substack{x=1\\(x,p)=1}}^{p^m} \chi(x^l(Ax^k+B)^w), \quad \sum_{x=1}^{p^m} \chi_1(x)\chi_2(Ax^k+B),$$

have a simple evaluation for large enough m (for $m \geq 2$ if $p \nmid ABk$).

1. Introduction

For an odd prime p and multiplicative character χ mod p^m we are interested in explicitly evaluating complete pure character sums of the form

$$S^*(\chi, x^l(Ax^k+B)^w, p^m) = \sum_{\substack{x=1\\p\nmid x}}^{p^m} \chi(x^l(Ax^k+B)^w) \tag{1.1}$$

once m is sufficiently large. Equivalently, for characters χ_1 and $\chi_2 \bmod p^m$ we consider the sums

$$S(\chi_1, \chi_2, Ax^k+B, p^m) = \sum_{x=1}^{p^m} \chi_1(x)\chi_2(Ax^k+B). \tag{1.2}$$

Writing

$$\chi_1 = \chi^l, \;\; \chi_2 = \chi^w, \quad \chi_1(x)\chi_2(Ax^k+B) = \chi(x^l(Ax^k+B)^w), \tag{1.3}$$

Manuscrit reçu le 13 avril 2013, révisé le 27 mars 2015, accepté le 15 avril 2015.
Mathematics Subject Classification. 11L10, 11L40, 11L03,11L05.
Mots-clefs. Character Sums, Gauss sums, Jacobi Sums.
The authors thank the referee for his careful reading of the original manuscript.

with $\chi_1 = \chi_0$ the principal character if $l = 0$, the correspondence between (1.1) and (1.2) is clear. These sums include the mod p^m generalizations of the classical Jacobi sums

$$J(\chi_1, \chi_2, p^m) = \sum_{x=1}^{p^m} \chi_1(x)\chi_2(1-x), \tag{1.4}$$

which have been evaluated exactly by Zhang Wenpeng & Weili Yao [20] when χ_1, χ_2 and $\chi_1\chi_2$ are primitive and $m \geq 2$ is even (some generalizations are considered in [19]).

More generally for a multiplicative character χ mod p^m, and rational functions $f(x), g(x) \in \mathbb{Z}(x)$ one can define the mixed complete exponential sum,

$$\mathscr{S}(\chi, g(x), f(x), p^m) := \sum_{x=1}^{p^m}{}^{*} \chi(g(x)) e_{p^m}(f(x)) \tag{1.5}$$

where $e_y(x) = e^{2\pi i x/y}$ and $*$ indicates that we omit any x producing a non-invertible denominator in f or g (as for example in (1.1) we must omit the $p \mid x$ if $l < 0$; for $l \geq 0$ the condition $p \nmid x$ is redundant unless $l = 0$, since the excluded terms are zero if $l > 0$). When $m = 1$ the Weil bound (see §4) is often the most that we can say about (1.5), but when $m \geq 2$ methods of Cochrane [3] (see also Cochrane and Zheng [5] & [7]) can sometimes be used to reduce and simplify the sums. For example we showed in [13] that the sums

$$\sum_{x=1}^{p^m} \chi(x) e_{p^m}(nx^k) \tag{1.6}$$

can be evaluated explicitly when m is sufficently large (for $m \geq 2$ if $p \nmid nk$). We show here that the sums (1.1) and (1.2) similarly have a simple evaluation for large enough m (for $m \geq 2$ if $p \nmid ABk$).

It is interesting that the sums (1.6) and (1.1) can both be written explicitly in terms of classical Gauss sums for any $m \geq 1$ (see §3). In particular one can trivially recover the Weil bound in these cases (see §4).

We shall assume throughout that χ_2 is a primitive character mod p^m (equivalently χ is primitive and $p \nmid w$). We assume, noting the correspondence (1.3) between (1.1) and (1.2), that

$$g(x) = x^l (Ax^k + B)^w, \quad p \nmid w \tag{1.7}$$

where k, l are integers with $k > 0$ (else $x \mapsto x^{-1}$) and A, B non-zero integers with

$$A = p^n A_1, \quad p \nmid A_1 B, \quad 0 \leq n < m. \tag{1.8}$$

We define the integers $d \geq 1$ and $t \geq 0$ by

$$d = (k, p-1), \qquad k = p^t k_1, \quad p \nmid k_1. \tag{1.9}$$

For $m \geq n + t + 1$ it transpires that the sum in (1.1) or (1.2) is zero unless

$$\chi_1 = \chi_3^k, \tag{1.10}$$

for some mod p^m character, χ_3 (i.e. χ is the $(k, \phi(p^m))/(k, l, \phi(p^m))$th power of a character), and we have a solution, x_0, to a characteristic equation of the form,

$$g'(x) \equiv 0 \bmod p^{\min\left\{m-1, \lceil \frac{m+n}{2} \rceil + t\right\}} \tag{1.11}$$

with

$$p \nmid x_0(Ax_0^k + B). \tag{1.12}$$

A solution to (1.11) satisfying (1.12) can be reduced to whether or or not a constant, dependent on χ_1, χ_2, k, A, and B, is a kth power mod a particular power of p (see (5.11)). Notice that in order to have a solution to (1.11) satisfying (1.12) we must have

$$l = p^{n+t} l_1, \quad p \nmid l_1, \quad p \nmid (p^n l_1 + w k_1), \tag{1.13}$$

if $m > t + n + 1$ (equivalently χ_1 is induced by a primitive mod p^{m-n-t} character and $\chi_1 \chi_2^k$ is a primitive mod p^{m-t} character) and $p^{n+t} \mid l$ if $m = t + n + 1$.

We shall use a to denote a primitive root mod p^m and define the integer r by

$$a^{p-1} = 1 + rp, \quad p \nmid r. \tag{1.14}$$

For the primitive character χ, with $\chi_1 = \chi^l$ and $\chi_2 = \chi^w$, we define an integer c by

$$\chi(a) = e_{\phi(p^m)}(c), \quad p \nmid c. \tag{1.15}$$

When (1.10) holds, (1.11) has a solution x_0 satisfying (1.12), and $m > n + t + 1$, we obtain the following explicit evaluation of the sum (1.2).

Theorem 1.1. *Suppose that p is an odd prime and $\chi_1 = \chi^l$, $\chi_2 = \chi^w$ are mod p^m characters with χ_2 primitive.*

If χ_1 satisfies (1.10)*, and* (1.11) *has a solution x_0 satisfying* (1.12)*, then*

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

$$= d\chi_1(x_0)\chi_2(Ax_0^k + B) \begin{cases} p^{m-1}, & \text{if } t + n + 1 < m \leq 2t + n + 2, \\ p^{\frac{m+n}{2} + t}, & \text{if } m > 2t + n + 2,\ m - n \text{ even}, \\ p^{\frac{m+n}{2} + t}\varepsilon_1, & \text{if } m > 2t + n + 2,\ m - n \text{ odd}, \end{cases}$$

except if $p = m - n = 3, t = 0, n > 0$ *when an extra factor* $e_3(-cl_1rk)$ *is needed, with*

$$\varepsilon_1 := \left(\frac{-2rc}{p}\right)\left(\frac{wl_1(p^n l_1 + wk_1)}{p}\right)\varepsilon, \qquad \varepsilon := \begin{cases} 1 & p \equiv 1 \ mod\ 4, \\ i & p \equiv 3 \ mod\ 4, \end{cases}$$

where n, d, t, k_1, l_1, r, c *and are as defined in* (1.8), (1.9), (1.13), (1.14), (1.15), *and* $\left(\frac{\alpha}{p}\right)$ *is the Legendre symbol.*

If χ_1 *does not satisfy* (1.10), *or* (1.11) *has no solution satisfying* (1.12), *then the sum is zero.*

From this we see that the non-zero sums have

$$\left|\sum_{x=1}^{p^m} \chi_1(x)\chi_2(Ax^k+B)\right| = \begin{cases} dp^{m-1}, & \text{if } t+n+1 < m \le 2t+n+2 \\ dp^{\frac{m+n}{2}+t}, & \text{if } 2t+n+2 < m. \end{cases} \tag{1.16}$$

For $t = 0$ the result (1.16) can be obtained from [3] by showing equality in their S_α evaluated at the d critical points α. For $t > 0$ the α will not have multiplicity one as needed in [3].

For the mod p^m Jacobi sums (1.4) we can take $x_0 = l(l+w)^{-1}$ and obtain:

Corollary 1.2. *Suppose that* p *is an odd prime and* $\chi_1 = \chi^l$, $\chi_2 = \chi^w$ *are mod* p^m *characters with* χ_2 *primitive.*
If $p \nmid l(l+w)$, *then*

$$J(\chi_1, \chi_2, p^m) = \frac{\chi_1(l)\chi_2(w)}{\chi_1\chi_2(l+w)} p^{\frac{m}{2}} \begin{cases} 1, & \textit{if } m \textit{ is even,} \\ \left(\frac{-2rc}{p}\right)\left(\frac{lw(l+w)}{p}\right)\varepsilon, & \textit{if } m \ge 3 \textit{ is odd.} \end{cases}$$

If $p \mid l(l+w)$, *then* $J(\chi_1, \chi_2, p^m) = 0$.

2. Preliminaries

Condition (1.10) will arise naturally in our proof of Theorem 1.1 but can also be seen from elementary considerations.

Lemma 2.1. *For any odd prime* p, *multiplicative characters* χ_1, χ_2 *mod* p^m, *and* f_1, f_2 *in* $\mathbb{Z}[x]$, *the sum* $S = \sum_{x=1}^{p^m} \chi_1(x)\chi_2(f_1(x^k))e_{p^m}(f_2(x^k))$ *is zero unless* $\chi_1 = \chi_3^k$ *for some mod* p^m *character* χ_3.

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

$$S = \sum_{x=1}^{p^m} \chi_1(xz)\chi_2(f_1((xz)^k))e_{p^m}(f_2((xz)^k)) = \chi_1(z)S.$$

Hence if $S \neq 0$ we must have $1 = \chi_1(z) = \chi_1(a)^{\phi(p^m)/(k,\phi(p^m))}$ and $\chi_1(a) = e_{\phi(p^m)}\left(c'(k,\phi(p^m))\right)$ for some integer c'. For an integer c_1 satisfying

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

we equivalently have $\chi_1 = \chi_3^k$ where $\chi_3(a) = e_{\phi(p^m)}(c_1)$. □

We remark that the restriction to primitive χ_2 is fairly natural; if χ_2 is not primitive but χ_1 is primitive then $S(\chi_1,\chi_2,Ax^k+B,p^m) = 0$ (since $\sum_{y=1}^{p}\chi_1(x+yp^{m-1}) = 0$), if both are not primitive we can reduce to a lower modulus

$$S(\chi_1,\chi_2,Ax^k+B,p^m) = pS(\chi_1,\chi_2,Ax^k+B,p^{m-1}).$$

The condition $m > t+n+1$ is also unsurprising; if $t \geq m-n$ then one can of course use Euler's Theorem to reduce the power of p in k to $t = m-n-1$. If $t = m-n-1$ and the sum is non-zero then, as in a Heilbronn sum, we obtain a mod p sum, $p^{m-1}\sum_{x=1}^{p-1}\chi(x^l(Ax^k+B)^w)$, where one does not expect a nice evaluation.

Finally we observe that if χ is a mod rs character with $(r,s)=1$, then $\chi = \chi_1\chi_2$ for a mod r character χ_1 and mod s character χ_2, and for any $g(x)$ in $\mathbb{Z}[x]$

$$\sum_{x=1}^{rs}\chi(g(x)) = \sum_{x=1}^{r}\chi_1(g(x))\sum_{x=1}^{s}\chi_2(g(x)).$$

Thus it is enough to work modulo prime powers.

3. Gauss Sums

For a character χ mod p^j, $j \geq 1$, we let $G(\chi,p^j)$ denote the classical Gauss sum

$$G(\chi,p^j) = \sum_{x=1}^{p^j}\chi(x)e_{p^j}(x).$$

Recall (see for example Section 1.6 of Berndt, Evans & Williams [1]) that

$$\left|G(\chi,p^j)\right| = \begin{cases} p^{j/2}, & \text{if } \chi \text{ is primitive mod } p^j, \\ 1, & \text{if } \chi = \chi_0 \text{ and } j = 1, \\ 0, & \text{otherwise.} \end{cases} \tag{3.1}$$

It is well known that the mod p Jacobi sums (1.4) (and their generalization to finite fields) can be written in terms of Gauss sums (see for example Theorem 2.1.3 of [1] or Theorem 5.21 of [11]). This extends to the mod p^m sums. For example when χ_1, χ_2 and $\chi_1\chi_2$ are primitive mod p^m

$$J(\chi_1,\chi_2,p^m) = \frac{G(\chi_1,p^m)G(\chi_2,p^m)}{G(\chi_1\chi_2,p^m)}, \tag{3.2}$$

and $|J(\chi_1,\chi_2,p^m)| = p^{m/2}$ (see Lemma 1 of [21] or [19]; the relationship for Jacobi sums over more general residue rings modulo prime powers can be found in [15]).

We showed in [13] that for $p\nmid n$ the sums

$$\mathscr{S}(\chi,x,nx^k,p^m)=\sum_{x=1}^{p^m}\chi(x)e_{p^m}(nx^k)$$

are zero unless $\chi=\chi_1^k$ for some character χ_1 mod p^m, in which case (summing over the characters whose order divides $(k,\phi(p^m))$ to pick out the kth powers)

$$\mathscr{S}(\chi,x,nx^k,p^m)=\sum_{\chi_2^{(k,\phi(p^m))}=\chi_0}\overline{\chi_1\chi_2}(n)G(\chi_1\chi_2,p^m). \tag{3.3}$$

From Lemma 2.1 we know that the sum in (1.2) is zero unless $\chi_1=\chi_3^k$ for some character χ_3 mod p^m, in which case the sum can be written as $(k,\phi(p^m))$ mod p^m Jacobi like sums $\sum_{x=1}^{p^m}\chi_5(x)\chi_2(Ax+B)$ and again be expressed in terms of Gauss sums.

Theorem 3.1. *Let p be an odd prime. If χ_1, χ_2 are characters mod p^m with χ_2 primitive and $\chi_1=\chi_3^k$ for some character χ_3 mod p^m, and n and A_1 are as defined in* (1.8)*, then*

$$\sum_{x=1}^{p^m}\chi_1(x)\chi_2(Ax^k+B)$$
$$= p^n\sum_{\chi_4\in X}\overline{\chi_3\chi_4}(A_1)\chi_2\chi_3\chi_4(B)\frac{G(\chi_3\chi_4,p^{m-n})G(\overline{\chi_2\chi_3\chi_4},p^m)}{G(\overline{\chi_2},p^m)},$$

where X denotes the mod p^m characters χ_4 with $\chi_4^D=\chi_0$, $D=(k,\phi(p^m))$, such that $\chi_3\chi_4$ is a mod p^{m-n} character.

Notice that if $(k,\phi(p^m))=1$, as in the generalized Jacobi sums (1.4), with χ_2 primitive, and $\chi_1=\chi_3^k$ is a mod p^{m-n} character if $p\mid A$, then we have the single $\chi_4=\chi_0$ term and

$$\sum_{x=1}^{p^m}\chi_1(x)\chi_2(Ax^k+B)=p^n\overline{\chi}_3(A_1)\chi_2\chi_3(B)\frac{G(\chi_3,p^{m-n})G(\overline{\chi_2\chi_3},p^m)}{G(\overline{\chi_2},p^m)},$$

of absolute value $p^{(m+n)/2}$ if $\chi_2,\chi_2\chi_3$ and χ_3 are primitive mod p^m and p^{m-n} (noting that $\overline{G(\overline{\chi},p^m)}=\chi(-1)G(\chi,p^m)$ we plainly recover the form (3.2) in that case).

For the multiplicative analogue of the classical Kloostermann sums, χ assumed primitive and $p\nmid A$, Theorem 3.1 gives a sum of two terms of size $p^{m/2}$

$$\sum_{x=1}^{p^m}{}^{*}\,\chi(Ax+x^{-1})=\frac{\overline{\chi}_3(A)}{G(\overline{\chi},p^m)}\left(G(\chi_3,p^m)^2+\chi^*(A)G\left(\chi_3\chi^*,p^m\right)^2\right)$$

when $\chi=\overline{\chi}_3^2$ (otherwise the sum is zero), where χ^* denotes the mod p^m extension of the Legendre symbol (taking $\chi_2=\chi$, $\chi_1=\overline{\chi}$, $k=2$ we have $D=2$ and $\chi_4=\chi_0$ or χ^*). For $m=1$ this is Han Di's [9, Lemma 1]. Cases where we can write the exponential sum explicitly in terms of Gauss sums seem rare. Best known (after the quadratic Gauss sums) are perhaps the Salié sums, evaluated by Salié [14] for $m=1$ (see Williams [18],[17] or Mordell [12] for a short proof) and Cochrane & Zheng [6, §5] for $m\geq 2$; for $p\nmid AB$

$$\begin{aligned}\sum_{x=1}^{p^m}{}^{*}\,&\chi^*(x)e_{p^m}(Ax+Bx^{-1})\\ &=\chi^*(B)\begin{cases}p^{\frac{1}{2}(m-1)}(e_{p^m}(2\gamma)+e_{p^m}(-2\gamma))G\left(\chi^*,p\right), & m\text{ odd},\\ p^{\frac{1}{2}m}\left(\chi^*(\gamma)e_{p^m}(2\gamma)+\chi^*(-\gamma)e_{p^m}(-2\gamma)\right), & m\text{ even},\end{cases}\end{aligned}$$

if $AB=\gamma^2 \bmod p^m$, and zero if $\chi^*(AB)=-1$. Cochrane & Zheng's $m\geq 2$ method works with a general χ as long as the congruence $rAx^2+cx-Br\equiv 0 \bmod p$ does not have a repeat root, but formulae seem lacking when $m=1$ and $\chi\neq\chi^*$. Explicit formulae for power moments of Kloosterman sums modulo prime powers are obtained in [8].

For the Jacobsthal sums we get (essentially Theorems 6.1.14 & 6.1.15 of [1])

$$\sum_{m=1}^{p-1}\left(\frac{m}{p}\right)\left(\frac{m^k+B}{p}\right)=\left(\frac{B}{p}\right)\sum_{j=0}^{k-1}\chi(B)^{2j+1}\frac{G(\chi^{2j+1},p)G(\overline{\chi}^{2j+1}\chi^*,p)}{G(\chi^*,p)},$$

$$\sum_{m=0}^{p-1}\left(\frac{m^k+B}{p}\right)=\left(\frac{B}{p}\right)\sum_{j=1}^{k-1}\chi(B)^{2j}\frac{G(\chi^{2j},p)G(\overline{\chi}^{2j}\chi^*,p)}{G(\chi^*,p)},$$

when $p\equiv 1 \bmod 2k$ and $p\nmid B$, where χ denotes a mod p character of order $2k$ and χ^* the mod p character corresponding to the Legendre symbol (see also [10]).

Proof of Theorem 3.1. Observe that if χ is a primitive character mod p^j, $j\geq 1$, then

$$\sum_{y=1}^{p^j}\chi(y)e_{p^j}(Ay)=\overline{\chi}(A)G(\chi,p^j). \tag{3.4}$$

Indeed, for $p \nmid A$ this is plain from $y \mapsto A^{-1}y$. If $p \mid A$ and $j=1$ the sum equals $\sum_{y=1}^{p} \chi(y) = 0$ and for $j \geq 2$ writing $y = a^{u+\phi(p^{j-1})v}$, a a primitive root mod p^m, $\chi(a) = e_{\phi(p^j)}(c)$, $u = 1, ..., \phi(p^{j-1})$, $v = 1, .., p$,

$$\sum_{y=1}^{p^j} \chi(y) e_{p^j}(Ay) = \sum_{u=1}^{\phi(p^{j-1})} \chi(a^u) e_{p^j}(Aa^u) \sum_{v=1}^{p} e_p(cv) = 0. \tag{3.5}$$

Hence if χ_2 is a primitive character mod p^m we have

$$G(\overline{\chi_2}, p^m)\chi_2(Ax^k+B) = \sum_{y=1}^{p^m} \overline{\chi_2}(y) e_{p^m}((Ax^k+B)y)$$

and, since $\chi_1 = \chi_3^k$ and $D = (k, \phi(p^m))$,

$$\begin{aligned}
G(\overline{\chi_2}, p^m) &\sum_{x=1}^{p^m} \chi_1(x)\chi_2(Ax^k+B) \\
&= \sum_{x=1}^{p^m} \chi_3(x^k) \sum_{y=1}^{p^m} \overline{\chi_2}(y) e_{p^m}((Ax^k+B)y) \\
&= \sum_{x=1}^{p^m} \chi_3(x^D) \sum_{y=1}^{p^m} \overline{\chi_2}(y) e_{p^m}((Ax^D+B)y) \\
&= \sum_{\chi_4^D=\chi_0} \sum_{u=1}^{p^m} \chi_3(u)\chi_4(u) \sum_{y=1}^{p^m} \overline{\chi_2}(y) e_{p^m}((Au+B)y) \\
&= \sum_{\chi_4^D=\chi_0} \sum_{y=1}^{p^m} \overline{\chi_2}(y) e_{p^m}(By) \sum_{u=1}^{p^m} \chi_3\chi_4(u) e_{p^m}(Auy) \\
&= \sum_{\chi_4^D=\chi_0} \sum_{y=1}^{p^m} \overline{\chi_2\chi_3\chi_4}(y) e_{p^m}(By) \sum_{u=1}^{p^m} \chi_3\chi_4(u) e_{p^m}(Au).
\end{aligned}$$

Since $p \nmid B$ we have

$$\sum_{y=1}^{p^m} \overline{\chi_2\chi_3\chi_4}(y) e_{p^m}(By) = \chi_2\chi_3\chi_4(B) G(\overline{\chi_2\chi_3\chi_4}, p^m).$$

If $\chi_3\chi_4$ is a mod p^{m-n} character then

$$\begin{aligned}
\sum_{u=1}^{p^m} \chi_3\chi_4(u) e_{p^m}(Au) &= p^n \sum_{u=1}^{p^{m-n}} \chi_3\chi_4(u) e_{p^{m-n}}(A_1 u) \\
&= p^n \overline{\chi_3\chi_4}(A_1) G(\chi_3\chi_4, p^{m-n}).
\end{aligned}$$

If $\chi_3\chi_4$ is a primitive character mod p^j for some $m-n<j\leq m$ then by (3.5)

$$\sum_{u=1}^{p^m}\chi_3\chi_4(u)e_{p^m}(Au)=p^{m-j}\sum_{u=1}^{p^j}\chi_3\chi_4(u)e_{p^j}(p^{j-(m-n)}A_1u)=0,$$

and the result follows. $\square$

Notice that if $m\geq n+2$ then by (3.1) the set X can be further restricted to those χ_4 with $\chi_3\chi_4$ primitive mod p^{m-n}. Hence if $p^t\,||\,k$, with $m\geq n+t+2$ and we write $\chi_3(a)=e_{\phi(p^m)}(c_3)$, $\chi_4(a)=e_{\phi(p^m)}(c_4)$ we have $p^{m-1-t}\mid c_4$, $p^n\,||\,(c_3+c_4)$, giving $p^n\,||\,c_3$. From $\chi_3^k=\chi_1=\chi^l$ this yields $p^{n+t}\,||\,c_3k=c_1=cl$ and $p^{n+t}\,||\,l$. If $n>0$ we deduce that $p^t\,||\,l+wk$. Moreover when $n=0$ reversing the roles of A and B gives $p^t\,||\,l+wk$. Hence when $m\geq n+t+2$ we have $S(\chi_1,\chi_2,Ax^k+B,p^m)=0$ unless (1.13) holds. For $m=n+t+1$ we similarly still have $p^{n+t}\mid l$.

4. Weil Bounds

For $m=1$ (non-degenerate) sums of the form (1.5) have Weil [16] type bounds; for example if f is a polynomial (with $f(x)$ not constant mod p or $g(x)\neq c\,h(x)^b$ where b is the order of χ) then

$$|\mathscr{S}(\chi,g(x),f(x),p)|\leq(\deg(f)+\ell-1)\,p^{1/2}, \tag{4.1}$$

where ℓ denotes the number of zeros and poles of g (see Castro & Moreno [2] or Cochrane & Pinner [4] for a treatment of the general case).

An expression in terms of Gauss sums will sometimes give us an elementary way of obtaining a Weil strength bound. For example from (3.3) one immediately obtains

$$\left|\mathscr{S}(\chi,x,nx^k,p^m)\right|\leq(k,\phi(p^m))p^{m/2}.$$

Similarly from Theorem 3.1 we have

$$\left|S(\chi_1,\chi_2,Ax^k+B,p^m)\right|\leq(k,\phi(p^m))p^{(m+n)/2}. \tag{4.2}$$

For $m=1$ and $p\nmid A$ this gives us the bound

$$\left|\sum_{x=1}^{p-1}\chi\left(x^l(Ax^k+B)^w\right)\right|\leq dp^{\frac{1}{2}},$$

where $d=(k,p-1)$. For $l=0$ we can slightly improve this for the complete sum,

$$\left|\sum_{x=0}^{p-1}\chi(Ax^k+B)\right|\leq(d-1)p^{\frac{1}{2}},$$

since, taking $\chi_1=\chi_3=\chi_0$, $\chi_2=\chi$, the $\chi_4=\chi_0$ term in Theorem 3.1 equals $-\chi(B)$, the missing $x=0$ term in (1.1). These correspond to the classical Weil bound (4.1) after an appropriate change of variables to replace k by d. For $m\geq t+1$ the bound (4.2) is $dp^{\frac{m+n}{2}+t}$, so by (1.16) we have equality in (4.2) for $m\geq n+2t+2$, but not for $t+n+1<m<2t+n+2$ (note $\frac{m+n}{2}+t=m-1$ when $m=n+2t+2$).

5. Proof of The Evaluation

Proof of Theorem 1.1. Let a be a primitive root mod p^m and define the integers r_l, $p\nmid r_l$, by

$$a^{\phi(p^l)}=1+r_lp^l,$$

so that $r=r_1$. Since $(1+r_{s+1}p^{s+1})=(1+r_sp^s)^p$, for any $s\geq 1$ we have

$$r_{s+1}\equiv r_s \bmod p^s. \tag{5.1}$$

We define the integers $c_1:=cl$, $c_2:=cw$, so that

$$\chi_1(a)=e_{\phi(p^m)}(c_1),\quad \chi_2(a)=e_{\phi(p^m)}(c_2). \tag{5.2}$$

Since χ_2 is assumed primitive we have $p\nmid c_2$.

We write

$$\gamma=u\frac{\phi(p^L)}{d}+v,\qquad L:=\begin{cases}1, & \text{if } m\leq n+2t+2,\\ \lceil\frac{m-n}{2}\rceil-t, & \text{if } m>n+2t+2,\end{cases}$$

and observe that if $u=1,...,dp^{m-L}$ and v runs through an interval I of length $\phi(p^L)/d$ then γ runs through a complete set of residues mod $\phi(p^m)$. Hence setting $h(x)=Ax^k+B$ and writing $x=a^\gamma$ we have

$$\sum_{x=1}^{p^m}\chi_1(x)\chi_2(h(x))=\sum_{v\in I}\chi_1(a^v)\sum_{u=1}^{dp^{m-1}}\chi_1(a^{u\frac{\phi(p^L)}{d}})\chi_2\left(h\left(a^{u\frac{\phi(p^L)}{d}+v}\right)\right).$$

Since $2(L+t)+n\geq m$ we can write

$$\begin{aligned} h\left(a^{u\frac{\phi(p^L)}{d}+v}\right)&=A\left(a^{\phi(p^{L+t})}\right)^{u\left(\frac{k}{dp^t}\right)}a^{vk}+B\\ &=A\left(1+r_{L+t}p^{L+t}\right)^{u\left(\frac{k}{dp^t}\right)}a^{vk}+B\\ &\equiv h(a^v)+A_1u\left(\frac{k}{dp^t}\right)a^{vk}r_{L+t}p^{L+t+n} \bmod p^m.\end{aligned}$$

This is zero mod p if $p \mid h(a^v)$ and consequently any such v give no contribution to the sum. If $p \nmid h(a^v)$ then, since $r_{L+t} \equiv r_{L+t+n} \bmod p^{L+t}$,

$$h\left(a^{u\frac{\phi(p^L)}{d}+v}\right) \equiv h(a^v)\left(1+A_1 u\left(\frac{k}{dp^t}\right)h(a^v)^{-1}a^{vk}r_{L+t+n}p^{L+t+n}\right) \bmod p^m$$

$$\equiv h(a^v)a^{A_1 u\left(\frac{k}{dp^t}\right)h(a^v)^{-1}a^{vk}\phi(p^{L+t+n})} \bmod p^m.$$

Thus, $\sum_{x=1}^{p^m} \chi_1(x)\chi_2(h(x))$ equals

$$\sum_{\substack{v\in I \\ p\nmid h(a^v)}} \chi_1(a^v)\chi_2(h(a^v)) \sum_{u=1}^{dp^{m-L}} \chi_1\left(a^{u\frac{\phi(p^L)}{d}}\right)\chi_2\left(a^{u\frac{\phi(p^L)}{d}Aka^{vk}h(a^v)^{-1}}\right),$$

where the inner sum $\sum_{u=1}^{dp^{m-L}} e_{dp^{m-L}}\left(u\left(c_1+c_2Ah(a^v)^{-1}ka^{vk}\right)\right)$ is dp^{m-L} if

$$c_1 + c_2 h(a^v)^{-1}A_1 a^{vk}\left(\frac{k}{dp^t}\right)dp^{t+n} \equiv 0 \bmod dp^{m-L} \tag{5.3}$$

and zero otherwise. Thus our sum will be zero unless (5.3) has a solution v with $p \nmid h(a^v)$. For $m \geq n+t+1$ we have $m-L \geq t+n$ and a solution to (5.3) necessitates $dp^{t+n} \mid c_1$ (giving us condition (1.10)) with $p^{t+n} \parallel l$ for $m > n+t+1$. Hence for $m > n+t+1$ we can simplify the congruence to

$$h(a^v)\left(\frac{c_1}{dp^{t+n}}\right) + c_2 A_1 a^{vk}\left(\frac{k}{dp^t}\right) \equiv 0 \bmod p^{m-L-t-n} \tag{5.4}$$

and for a solution we must have $p^t \parallel c_1 + kc_2$. Equivalently,

$$\frac{cg'(a^v)}{dp^{t+n}} \equiv 0 \bmod p^{m-t-n-L}, \tag{5.5}$$

and we must have a solution x_0 to

$$g'(x) \equiv 0 \bmod p^{\min\left\{m-1,\, \lfloor\frac{m+n}{2}\rfloor+t\right\}} \tag{5.6}$$

satisfying (1.12). Suppose that (5.6) has a solution $x_0 = a^{v_0}$ with $p \nmid h(x_0)$ and that $m > n+t+1$. Rewriting the congruence (5.5) in terms of the primitive root, a, gives

$$a^{vk} \equiv a^b \bmod p^{m-t-n-L}$$

for some integer b. Thus two solutions to (5.5), a^{v_1} and a^{v_2} must satisfy

$$v_1 k \equiv v_2 k \bmod \phi(p^{m-t-n-L}).$$

That is $v_1 \equiv v_2 \bmod \frac{(p-1)}{d}$ if $m \leq n+2t+2$ and if $m > n+2t+2$

$$v_1 \equiv v_2 \bmod \frac{\phi(p^{m-n-2t-L})}{d}$$

where $m-n-2t-L = L$ if $m-n$ is even and $L-1$ if $m-n$ is odd. Thus if $n+t+1 < m \leq n+2t+2$ or $m > n+2t+2$ and $m-n$ is even our interval I contains exactly one solution v. Choosing I to contain v_0 we get that

$$\sum_{x=1}^{p^m} \chi_1(x)\chi_2(h(x)) = dp^{m-L}\chi_1(x_0)\chi_2(h(x_0)).$$

Suppose that $m > n+2t+2$ with $m-n$ odd and set $s := \frac{m-n-1}{2}$. In this case I will contain p solutions and we pick our interval I to contain the p solutions $v_0 + yp^{s-t-1}\left(\frac{p-1}{d}\right)$ where $y = 0, \dots, p-1$. Since $dp^t \mid c_1$ and $dp^t \mid k$ we can write, with g defined as in (1.7),

$$g_1(x) := g(x)^c = x^{c_1}(Ax^k+B)^{c_2} =: H\left(x^{dp^t}\right).$$

Thus, setting $\chi = \chi_4^c$, where χ_4 is the mod p^m character with $\chi_4(a) = e_{\phi(p^m)}(1)$,

$$\begin{aligned}\sum_{x=1}^{p^m} \chi_1(x)\chi_2(h(x)) &= dp^{\frac{m+n-1}{2}+t}\sum_{y=0}^{p-1}\chi\left(g\left(a^{v_0+yp^{s-t-1}\left(\frac{p-1}{d}\right)}\right)\right)\\ &= dp^{\frac{m+n-1}{2}+t}\sum_{y=0}^{p-1}\chi_4\left(H\left(x_0^{dp^t}a^{y\phi(p^s)}\right)\right),\end{aligned}$$

where

$$x_0^{dp^t}a^{y\phi(p^s)} = x_0^{dp^t}(1+r_sp^s)^y = x_0^{dp^t} + yr_sx_0^{dp^t}p^s \bmod p^{m-n-1}. \tag{5.7}$$

If $n=0$ then $3s \geq m$. If $n>0$ then, since

$$p^{-n}H'(x^{dp^t}) = \left(\frac{xg_1'(x)}{dp^{t+n}}\right)x^{-dp^t} \in \mathbb{Z}[x],$$

we have $p^n \mid \frac{1}{(k-1)!}H^{(k)}\left(x_0^{dp^t}\right)$, and $p^{n-v_p(k)} \mid \frac{1}{k!}H^{(k)}\left(x_0^{dp^t}\right)$ for all $k \geq 1$ where $v_p(k)$ is the p-adic valuation of k, $p^{v_p(k)} \,||\, k$. Since $v_p(k) \leq \log k/\log p$ we have

$$\mathcal{B}(k) := ks+n-v_p(k) \geq ks - \frac{\log k}{\log p} + n \geq 3s - \frac{\log 3}{\log p} + n = m+s-1-\frac{\log 3}{\log p} \geq m$$

for all $k \geq 3$ if $m-n \geq 5$. For $m-n=3$ we have $\mathcal{B}(4) = m+1$ and for $k \geq 5$, $\mathcal{B}(k) \geq 5+m-3-\log 5/\log p > m$ for all $p \geq 3$ with $\mathcal{B}(3) = m$ for

$p \geq 5$. Hence, excluding the case $p = 3 = m - n$, $n > 0$, $t = 0$ we have

$$(p^s)^k \frac{H^{(k)}\left(x_0^{dp^t}\right)}{k!} \equiv 0 \bmod p^m, \tag{5.8}$$

for all $k \geq 3$. For $p = 3 = m - n$, $n > 0$, $t = 0$ congruence (5.8) holds for $k \geq 4$ while it is easily checked that $H'''(x) \equiv -(c_1/d3^n)B^{c_2}x^{c_1/d-3}3^n$ mod 3^{n+1} and

$$\frac{1}{3!}H'''(x_0^d)\left(yr_s x_0^d p^s\right)^3 \equiv (c_1/d3^n)g_1(x_0)r_s y 3^{m-1} \bmod 3^m.$$

As $xg_1'(x) = (c_1 + kc_2)g_1(x) - c_2kBg_1(x)/h(x)$,

$$\begin{aligned} p^{-n}H''(x^{dp^t})x^{2dp^t} &= \left(\frac{c_1}{dp^t} + c_2\frac{k}{dp^t} - c_2\frac{k}{dp^t}\frac{B}{h(x)} - 1\right)\left(\frac{xg_1'(x)}{dp^{t+n}}\right) \\ &\qquad + c_2\left(\frac{k}{dp^t}\right)^2 A_1Bx^k\frac{g_1(x)}{h(x)^2}. \end{aligned}$$

Plainly a solution x_0 to (5.6) satisfying (1.12) also has $g_1'(x_0) \equiv 0$ mod $p^{\frac{m+n-1}{2}+t}$ and

$$\frac{x_0g_1'(x_0)}{dp^{t+n}} = \lambda p^{\frac{m-n-1}{2}}, \qquad H'(x_0^{dp^t}) = x_0^{-dp^t}\lambda p^{\frac{m+n-1}{2}}, \tag{5.9}$$

for some integer λ, and

$$p^{-n}H''(x_0^{dp^t}) \equiv c_2\left(\frac{k}{dp^t}\right)^2 A_1Bx_0^{k-2dp^t}\frac{g_1(x_0)}{h(x_0)^2} \bmod p.$$

Hence by the Taylor expansion, using (5.7) and that $r_s \equiv r_{m-1} \equiv r \bmod p$,

$$\begin{aligned} H\left(x_0^{dp^t}a^{y\phi(p^s)}\right) &\equiv H(x_0^{dp^t}) + H'(x_0^{dp^t})yr_sx_0^{dp^t}p^{\frac{m-n-1}{2}} \\ &\qquad + 2^{-1}H''(x_0^{dp^t})y^2r_s^2x_0^{2dp^t}p^{m-n-1} \bmod p^m \\ &\equiv g_1(x_0)\left(1 + \left(\beta y + \alpha y^2\right)r_{m-1}p^{m-1}\right) \bmod p^m \\ &\equiv g_1(x_0)a^{(\beta y + \alpha y^2)\phi(p^{m-1})} \bmod p^m, \end{aligned}$$

with

$$\beta := g_1(x_0)^{-1}\lambda, \qquad \alpha := 2^{-1}c_2h(x_0)^{-2}rA_1B\left(\frac{k}{dp^t}\right)^2 x_0^k, \tag{5.10}$$

unless $p = 3 = m - n$, $n > 0$, $t = 0$ when the additional term in the expansion gives $\beta := g_1(x_0)^{-1}\lambda + (c_1/d3^n)$, and

$$\chi_4\left(H\left(x_0^{dp^t}a^{y\phi(p^s)}\right)\right) = \chi(g(x_0))e_p(\alpha y^2 + \beta y).$$

Since plainly $p \nmid \alpha$, completing the square then gives

$$\begin{aligned}\sum_{x=1}^{p^m} \chi_1(x)\chi_2(h(x)) &= dp^{\frac{m+n-1}{2}+t}\chi(g(x_0))e_p(-4^{-1}\alpha^{-1}\beta^2)\sum_{y=0}^{p-1} e_p(\alpha y^2)\\ &= dp^{\frac{m+n-1}{2}+t}\chi(g(x_0))e_p(-4^{-1}\alpha^{-1}\beta^2)\left(\frac{\alpha}{p}\right)\varepsilon p^{\frac{1}{2}}\end{aligned}$$

where ε is 1 or i as p is 1 or 3 mod 4.

Notice that $g'(x_0) \equiv 0 \bmod p^{\frac{m+n-1}{2}+t}$ corresponds to

$$x_0^k \equiv -BA_1^{-1}l_1(wk_1+p^n l_1)^{-1} \bmod p^{\frac{m-n-1}{2}}. \tag{5.11}$$

Hence, since it is unchanged by a square mod p, we can replace the α inside the Legendre symbol by $2cwrA_1Bx_0^k$, and the x_0^k by $-A_1Bl_1(wk_1+p^nl_1)$, giving

$$\left(\frac{\alpha}{p}\right) = \left(\frac{-2rcwl_1(wk_1+p^nl_1)}{p}\right).$$

Observe that $x^k \equiv a^\gamma \bmod p^l$ has a solution if and only if $(k, \phi(p^l)) \mid \gamma$. In particular for $l-1 \geq t$ a solution mod p^l guarantees a solution mod p^{l+1}. Since $\frac{m-n-1}{2}-1 \geq t$, it is clear from the form (5.11) that (5.6) has a solution satisfying (1.12) if and only if (1.11) does. For such a solution x_0 we have $p \mid \lambda$ and $e_p(-4^{-1}\alpha^{-1}\beta^2)=1$ (unless $p=3=m-n$, $n>0$, $t=0$ when $-4^{-1}\alpha^{-1}\beta^2 \equiv -\alpha \equiv -rcl_1k \bmod 3$). □

References

[1] B. C. BERNDT, R. J. EVANS & K. S. WILLIAMS, *Gauss and Jacobi sums*, Canadian Mathematical Society Series of Monographs and Advanced Texts, John Wiley & Sons, Inc., New York, 1998, A Wiley-Interscience Publication, xii+583 pages.

[2] F. N. CASTRO & C. J. MORENO, "Mixed exponential sums over finite fields", *Proc. Amer. Math. Soc.* **128** (2000), no. 9, p. 2529-2537.

[3] T. COCHRANE, "Exponential sums modulo prime powers", *Acta Arith.* **101** (2002), no. 2, p. 131-149.

[4] T. COCHRANE & C. PINNER, "Using Stepanov's method for exponential sums involving rational functions", *J. Number Theory* **116** (2006), no. 2, p. 270-292.

[5] T. COCHRANE & Z. ZHENG, "Pure and mixed exponential sums", *Acta Arith.* **91** (1999), no. 3, p. 249-278.

[6] ———, "Exponential sums with rational function entries", *Acta Arith.* **95** (2000), no. 1, p. 67-95.

[7] ———, "A survey on pure and mixed exponential sums modulo prime powers", in *Number theory for the millennium, I (Urbana, IL, 2000)*, A K Peters, Natick, MA, 2002, p. 273-300.

[8] K. GONG, W. VEYS & D. WAN, "Power moments of Kloosterman sums", `http://arxiv.org/abs/1306.4104`.

[9] D. HAN, "A hybrid mean value involving two-term exponential sums and polynomial character sums", *Czechoslovak Math. J.* **64(139)** (2014), no. 1, p. 53-62.

[10] P. A. LEONARD & K. S. WILLIAMS, "Evaluation of certain Jacobsthal sums", *Boll. Un. Mat. Ital. B (5)* **15** (1978), no. 3, p. 717-723.

[11] R. LIDL & H. NIEDERREITER, *Finite fields*, second ed., Encyclopedia of Mathematics and its Applications, vol. 20, Cambridge University Press, Cambridge, 1997, With a foreword by P. M. Cohn, xiv+755 pages.

[12] L. J. Mordell, "On Salié's sum", *Glasgow Math. J.* **14** (1973), p. 25-26.
[13] V. Pigno & C. Pinner, "Twisted monomial Gauss sums modulo prime powers", *Funct. Approx. Comment. Math.* **51** (2014), no. 2, p. 285-301.
[14] H. Salié, "Über die Kloostermanschen Summen $S(u,v;q)$", *Math. Z.* **34** (1932), no. 1, p. 91-109.
[15] J. Wang, "On the Jacobi sums modulo P^n", *J. Number Theory* **39** (1991), no. 1, p. 50-64.
[16] A. Weil, "On some exponential sums", *Proc. Nat. Acad. Sci. U. S. A.* **34** (1948), p. 204-207.
[17] K. S. Williams, "Note on Salié's sum", *Proc. Amer. Math. Soc.* **30** (1971), p. 393-394.
[18] ———, "On Salié's sum", *J. Number Theory* **3** (1971), p. 316-317.
[19] W. Zhang & Z. Xu, "On the Dirichlet characters of polynomials in several variables", *Acta Arith.* **121** (2006), no. 2, p. 117-124.
[20] W. Zhang & W. Yao, "A note on the Dirichlet characters of polynomials", *Acta Arith.* **115** (2004), no. 3, p. 225-229.
[21] W. Zhang & Y. Yi, "On Dirichlet characters of polynomials", *Bull. London Math. Soc.* **34** (2002), no. 4, p. 469-473.

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

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