A note on evaluations of some exponential sums

by

Marko J. Moisio (Vaasa)

1. Introduction. The recent article [1] gives explicit evaluations for exponential sums of the form

\[ S(a, p^\alpha + 1) := \sum_{x \in \mathbb{F}_q} \chi(ax^{p^\alpha + 1}) \]

where \( \chi \) is a non-trivial additive character of the finite field \( \mathbb{F}_q \), \( q = p^e \) odd, and \( a \in \mathbb{F}_q^* \). In my dissertation [5], in particular in [4], I considered more generally the sums \( S(a, N) \) for all factors \( N \) of \( p^\alpha + 1 \). The aim of the present note is to evaluate \( S(a, N) \) in a short way, following [4]. We note that our result is also valid for even \( q \), and the technique used in our proof can also be used to evaluate certain sums of the form

\[ \sum_{x \in \mathbb{F}_q} \chi(ax^{p^\alpha + 1} + bx). \]

2. Evaluation of \( S(a, N) \). Let \( \mathbb{F}_q \) denote the finite field with \( q = p^e \) elements, \( \chi_1 \) the canonical additive character of \( \mathbb{F}_q \) and \( \alpha \) a non-negative integer. Let \( N \) be an arbitrary divisor of \( p^\alpha + 1 \). Our task is to evaluate the sums

\[ S(a, N) := \sum_{x \in \mathbb{F}_q} \chi_1(ax^N) \]

for non-zero elements \( a \) of \( \mathbb{F}_q \).

Let \( d = \gcd(\alpha, e) \). Since \( S(a, N) = S(a, \gcd(N, p^\alpha - 1)) \) and

\[ \gcd(p^\alpha + 1, p^\alpha - 1) = \begin{cases} 
1 & \text{if } e/d \text{ is odd and } p = 2, \\
2 & \text{if } e/d \text{ is odd and } p > 2, \\
p^d + 1 & \text{if } e/d \text{ is even,}
\end{cases} \]

as proved in [1] and [3, p. 175], it is enough to consider sums \( S(a, n) \) for all divisors \( n \) of \( p^d + 1 \). The case \( e/d \) odd is easily established (see [1]).

2000 Mathematics Subject Classification: Primary 11T24.
To state our result we fix a primitive element of $\mathbb{F}_q$, say $\gamma$, and denote the multiplicative group of $\mathbb{F}_q$ by $\mathbb{F}_q^*$.

**Theorem 1.** Let $e = 2sd$ and $n \mid p^d + 1$. Then

$$
\sum_{x \in \mathbb{F}_q^*} \chi_1(ax^n) = \begin{cases}
(-1)^s p^s & \text{if } \text{ind.}, \ a \not\equiv k \pmod{n}, \\
(-1)^s (n - 1)p^s & \text{if } \text{ind.}, \ a \equiv k \pmod{n},
\end{cases}
$$

where $k = 0$ if

(A) $p = 2$; or $p > 2$ and $2 \mid s$; or $p > 2$, $2 \nmid s$ and $2 \mid (p^d + 1)/n$,

and $k = n/2$ if

(B) $p > 2$, $2 \nmid s$ and $2 \nmid (p^d + 1)/n$.

In the special case $n = p^d + 1$, $p$ odd, our Theorem 1 gives Theorem 2 of [1].

The proof of our theorem is based on the relation (see [2, p. 217])

$$(1) \quad \sum_{x \in \mathbb{F}_q^*} \chi_1(ax^n) = \sum_{\psi \in H} G(\overline{\psi}) \psi(a)$$

where $H$ is the subgroup of order $n$ of the multiplicative character group of $\mathbb{F}_q$, and $G(\overline{\psi})$ is the Gauss sum

$$G(\overline{\psi}) = \sum_{x \in \mathbb{F}_q^*} \chi_1(x) \overline{\psi}(x).$$

**Proof of Theorem 1.** Let $H'$ be the subgroup of order $n$ of the multiplicative character group of $\mathbb{F}_{p^d}$. The surjectivity of the norm mapping $N$ from $\mathbb{F}_q$ to $\mathbb{F}_{p^d}$ implies $H = \{ \psi \circ N \mid \psi \in H' \}$. Now (1) and the Davenport–Hasse theorem (see [2, pp. 195–199]) imply

$$(2) \quad \sum_{x \in \mathbb{F}_q^*} \chi_1(ax^n) = \sum_{\psi \in H'} G(\overline{\psi} \circ N) \psi(N(a)) = (-1)^{s-1} \sum_{\psi \in H'} G'(\overline{\psi}) \psi(N(a)),$$

where $G'(\overline{\psi})$ is computed over $\mathbb{F}_{p^d}$.

Let $\psi_0$ denote the trivial multiplicative character of $\mathbb{F}_{p^d}$. Since $G'(\overline{\psi_0}) = -1$, it follows from (2) that

$$\sum_{x \in \mathbb{F}_q} \chi_1(ax^n) = (-1)^{s-1} \sum_{\psi \in H'} G'(\overline{\psi}) \psi(N(a)),$$

where $H'' := H' \setminus \{ \psi_0 \}$.

Let $\psi \in H''$. Since ord($\psi$) $\mid p^d + 1$, we observe that Stickelberger’s theorem (see [2, p. 202]) is applicable.

Now, if $p = 2$ or $2 \mid s$, then $G'(\overline{\psi}) = p^s$. To consider the remaining cases, we fix a generator of the multiplicative character group of $\mathbb{F}_{p^d}$, say $\lambda$, and define $t = (p^{2d} - 1)/n$. 
Now $\psi = \lambda^j$ for some $j \in \{1, \ldots, n-1\}$. Since $\text{ord}(\psi) = n/\gcd(n, j)$, we see that $(p^d + 1)/\text{ord}(\psi)$ is even if $(p^d + 1)/n$ is even. Consequently, $G'(\psi)^s = p^{sd}$ if $(p^d + 1)/n$ is even.

Thus in Case A we have

\[ \sum_{x \in \mathbb{F}_q} \chi_1(ax^n) = (-1)^{s-1}p^{sd} \sum_{j=1}^{n-1} \lambda^j(N(a)). \]

In Case B, $(p^d + 1)/\text{ord}(\psi)$ is even if and only if $j$ is even. Thus

\[ \sum_{x \in \mathbb{F}_q} \chi_1(ax^n) = (-1)^{s-1}p^{sd} \sum_{j=1}^{n-1} (-1)^j \lambda^j(N(a)). \]

Noting that $N(\gamma)$ is a primitive element of $\mathbb{F}_{p^{2d}}$, we easily obtain the result. □

If $n = p^d + 1$ and $s = 1$, for example, we can prove by a more or less similar reasoning (see [5])

**Theorem 2.** Let $a, b \in \mathbb{F}_q$, $b \neq 0$. Then

\[ \sum_{x \in \mathbb{F}_q} \chi_1(ax^{p^d+1} + bx) = \begin{cases} 0 & \text{if } a + a^{p^d} = 0, \\ -p^d\chi'_1(-b^{p^d+1}(a + a^{p^d})^{-1}) & \text{if } a + a^{p^d} \neq 0, \end{cases} \]

where $\chi'_1$ is the canonical additive character of the field $\mathbb{F}_{p^d}$.

**Acknowledgements.** The author is indebted to Professor Keijo Väänänen for his valuable comments on a preliminary version of this note.

**References**


Department of Mathematics and Statistics
University of Vaasa
Box 700, 65101 Vaasa, Finland
E-mail: mamo@uwasa.fi

Received on 11.8.1998
and in revised form on 30.12.1999