EXPLICIT EVALUATION
OF CERTAIN EXPONENTIAL SUMS

L. CARLITZ

1. Introduction.
Let \( F = \text{GF} (q) \) denote the finite field of order \( q = p^n, \) \( p \) prime, \( n \geq 1. \) For \( a \in F \) put
\[
t(a) = a + a^p + \ldots + a^{p^{n-1}}
\]
and
\[
e(a) = e^{2\pi i t(a)/p}.
\]
Define the exponential sums
\[
S(a, b) = \sum_{x \in F} e(ax^3 + bx)
\]
and
\[
T(a, b) = \sum_{x \in F} e(ax^6 + bx^2).
\]

In an earlier paper [1] the writer proved that, for \( p > 3, \) \( a \neq 0, \)
\[
\psi(3a)T(a, b)G = S^2(4a, b) + \psi(3a)S(a, b)G - q,
\]
where \( \psi(a) = +1, -1, 0 \) according as \( a \) is a nonzero square, a non-square or the zero element of \( F, \) and \( G \) is the Gauss sum defined by
\[
G = \sum_{x \in F} \psi(x)e(x).
\]
Since \( |G| = q^{1/4}, \) it follows from (1.3) that the two estimates
\[
S(a, b) = O(q^{1/4}), \quad T(a, b) = O(q^{1/4})
\]
are equivalent.

The case \( p = 3 \) is of little interest. We have
\[
S(a^3, b) = \begin{cases} q & (a + b = 0) \\ 0 & (a + b \neq 0) \end{cases},
\]

Received May 29, 1978.
\[ T(a^3, b) = \begin{cases} 
q & (a + b = 0) \\
\psi(a + b)G & (a + b \neq 0) 
\end{cases} \]

The case \( p = 2 \) is more interesting. Since \( e(a) = e(a^2) \) it follows that
\[ T(a^2, b^2) = S(a, b). \]

Also it is clear from the definition of \( e(a) \) that \( S(a, b) \) is now a rational integer. It is proved in [1] that, for \( q = 2^n \),
\[ S^2(a, b) = (1 - e(bu_0))q \quad (n \text{ odd}), \]
where \( u_0 \) is the unique solution of \( au^3 = 1 \). For \( n \) even we have
\[ S^2(a, b) = \begin{cases} 
q & (au^3 = 1 \text{ not solvable}) \\
(1 + e(bu_0) + e(bu_1) + e(bu_2))q & 
\end{cases} \]
where \( u_0, u_1, u_2 \) are the three solutions of \( au^3 = 1 \). It is assumed throughout that \( a \neq 0 \). The coefficient of \( q \) in the second half of (1.6) is equal to 0 or 4. Thus \( S(a, b) \) is evaluated except for sign.

The object of the present note is to determine the sign of \( S(a, b) \). The cases \( n \) even and \( n \) odd require separate treatment. We show in particular that, for \( n = 2m, a \in F, a \neq 0, \)
\[ S(a, 0) = \begin{cases} 
(-1)^m + 12^{m+1} & \\
(-1)^m 2^m & 
\end{cases} \]
according as \( a \) is or is not a cube in \( F \). For the general case, if \( a = c^3, c \in F, \) then
\[ S(c^3, b) = \begin{cases} 
(-1)^m + 12^{m+1}e(u_0^3) & \\
0 & 
\end{cases} \]
according as
\[ \sum_{j=0}^{m-1} (bc^{-1})^{2j} = 0 \]
is or is not satisfied; \( u_0 \) denote any solution of the equation \( u^4 + u = b^2c^{-2} \). If \( a \neq c^3, c \in F, \) then
\[ S(a, b) = (-1)^m 2^m e(ax_0^3), \]
where \( x_0 \) is the unique solution of \( a^2x^4 + ax = b^2 \).

For \( n = 2m + 1 \) it suffices to take \( b = 1 \). We show that
\[ S(1, 1) = \left( \frac{2}{2m+1} \right)^{2m+1}, \]
where \((2/2m+1)\) is the Jacobi symbol (quadratic character). If \(e(b) = -1\), we may put \(b = c^4 + c + 1\); then

\[
S(1, b) = e(c^3 + c) \left( \frac{2}{2m+1} \right)^{2^{m+1}}.
\]

Finally

\[
S(1, b) = 0 \quad (e(b) = +1).
\]

For a fuller statement of the results see Theorems 1 and 2 below.

2.

We consider first the case \(n\) even. Then \(3 \mid q - 1\). Let \(\chi\) denote a non-principal cubic character of the multiplicative group of the nonzero elements of \(F\). Define

\[
(2.1) \quad R(\chi) = \sum_{a \in F} \chi(a)e(a).
\]

We have

\[
|R(\chi)|^2 = R(\chi)R(\bar{\chi}) = \sum_{a, b} \chi(a)\bar{\chi}(b)e(a+b)
\]

\[
= \sum_{a, b} \chi(ab^2)e(a+b) = \sum_{a, b \neq 0} \chi(a)e(ab + b)
\]

\[
= \sum_a \chi(a) \sum_b e((a+1)b),
\]

so that

\[
(2.2) \quad |R(\chi)|^2 = q.
\]

Similarly

\[
R^2(\chi) = \sum_{a, b} \chi(ab)e(a+b) = \sum_{a, b \neq 0} \chi(a)e(ab^2 + b)
\]

\[
= \sum_a \chi(a) \sum_b e((a+1)b^2)
\]

and therefore

\[
(2.3) \quad R^2(\chi) = q.
\]

Comparison of (2.2) and (2.3) gives

\[
(2.4) \quad R(\chi) = R(\bar{\chi}),
\]

so that \(R(\chi)\) is a rational integer.

We now define the sums
\begin{equation}
S_0 = \frac{1}{3} \sum_{a \neq 0} e(a^3) \\
S_1 = \frac{1}{3} \sum_{a \neq 0} e(ba^3) \quad (\chi(b) = \omega) \\
S_2 = \frac{1}{3} \sum_{a \neq 0} e(ca^3) \quad (\chi(c) = \omega^2),
\end{equation}

where \( \omega = (1 + \sqrt{-3})/2 \). It is evident that \( S_0, S_1, S_2 \) are rational integers.

It follows from (2.1) and (2.5) that

\begin{equation}
-1 = S_0 + S_1 + S_2 \\
R(\chi) = S_0 + \omega S_1 + \omega S_1 + \omega^2 S_2 \\
R(\chi^2) = S_0 + \omega^2 S_1 + \omega S_2
\end{equation}

and

\begin{equation}
3S_0 = -1 + 2R(\chi) \\
3S_1 = -1 - R(\chi) \\
3S_2 = -1 - R(\chi).
\end{equation}

It is clear, by (2.3), that

\begin{equation}
R(\chi) = \pm 2^n \quad (n = 2m).
\end{equation}

By (2.7) we have

\begin{equation}
R(\chi) \equiv -1 \pmod{3},
\end{equation}

so that (2.8) becomes

\begin{equation}
R(\chi) = (-1)^{m-1}2^m.
\end{equation}

It then follows from (2.7) that

\begin{equation}
\begin{cases}
3S_0 = -1 + (-1)^{m-1}2^{m+1} \\
3S_1 = 3S_2 = -1 + (-1)^m 2^m.
\end{cases}
\end{equation}

The sum

\begin{equation}
S(a) = S(a, 0) = \sum_x e(ax^3) \quad (a \neq 0)
\end{equation}

can now be evaluated. Clearly

\begin{equation}
S(a) = \begin{cases}
1 + 3S_0 & (\chi(a) = 1) \\
1 + 3S_1 & (\chi(a) \neq 1).
\end{cases}
\end{equation}

Hence we have
\[ S(a) = \begin{cases} (-1)^{m-1}2^{m+1} & (\chi(a) = 1) \\ (-1)^m2^m & (\chi(a) \neq 1). \end{cases} \]

3.

The product
\[ S(a)S(a, b) = \sum_{x, y} e(ax^3 + a^2x^2y + by) \]
\[ = \sum_{x, y} e(a(x+y)^3 + ay^3 + by) \]
\[ = \sum_x e(ax^3) \sum_y e(ax^2y + axy^2 + by). \]

The inner sum is equal to
\[ \sum_y e((a^2x^4 + ax + b^2)y). \]

This sum vanishes unless
\[ a^2x^4 + ax = b^2. \]

There are two cases to consider according as \( a = c^3, c \in \text{GF}(q), \) or \( a \neq c^3). \) In the first case, (3.2) becomes
\[ u^4 + u = b^2c^{-2} \quad (u = cx). \]

This equation is solvable in \( \text{GF}(q) \) if and only if [2, p. 29]
\[ \sum_{j=0}^{m-1} (bc^{-1})^{2^{2j}} = 0 \quad (n=2m). \]

When (3.4) is satisfied, the four solutions of (3.3) are given by
\[ u_0, u_1 = u_0 + 1, u_0 + \theta, u_0 + \theta^2, \]
where \( u_0 \) is any solution of (3.3) and \( \theta \in \text{GF}(4), \theta^2 = \theta + 1. \)

Thus (3.1) becomes
\[ S(c^3)S(c^3, b) = q \sum_{u_i} e(u_i^3), \]
where the summation is over the four values (3.5). Now
\[ t((u_0 + 1)^3) = t(u_0^3) + t(u_0^2 + u_0) + t(1) = t(u_0^3) \]
\[ t((u_0 + \theta)^3) = t(u_0^3) + t(u_0^3 \theta + u_0 \theta^2) + t(1) = t(u_0^3), \]
so that (3.6) reduces to
\begin{equation}
S(c^3)S(c^3, b) = 4qe(u_0^3) = 2^{2m+2}e(u_0^3).
\end{equation}

Therefore, by the first of (2.13), we get
\begin{equation}
S(c^3, b) = (-1)^m12^{m+1}e(u_0^3)
\end{equation}

provided (3.4) is satisfied. If (3.4) is not satisfied, \(S(c^3, b) = 0\).

Returning to (3.2), assume now that \(a \neq c^3\), \(c \in \mathbb{GF}(q)\). Then, by (3.2),
\[
a^{2j}x^{2j+2} + x^{2j} = (a^{-1}b^2)^{2j} \quad (j = 0, 1, \ldots, m-1).
\]

Multiply both sides by
\[
a^1 + a^2 + \ldots + a^{2^j-2} = a^{(2^j-1)/3}
\]

and add the resulting equations:
\begin{equation}
(a^{(2^{2m}-1)/3} + 1)x = \sum_{j=0}^{m-1} (a^{-1}b^2)^{2j}a^{(2^j-1)/3}.
\end{equation}

Since \(a \neq c^3\), the coefficient of \(x\) does not vanish; moreover it is easily verified that the value of \(x\) given by (3.9) satisfies (3.2). Let \(x_0\) denote this value. Then (3.1) gives
\begin{equation}
S(a)S(a, b) = qe(ax_0^3) = 2^{2m}e(ax_0^3).
\end{equation}

Hence by the second of (2.13), (3.10) reduces to
\begin{equation}
S(a, b) = (-1)^m2^{m}e(ax_0^3) \quad (\chi(a) = 1).
\end{equation}

Summing up the results of section 2, 3, we state the following

**Theorem 1.** Let \(q = 2^m\), \(a, b \in \mathbb{GF}(q)\), \(a \neq 0\), \(b \neq 0\),
\[
S(a, b) = \sum_{x \in \mathbb{GF}(q)} e(ax^2 + bx), \quad S(a) = S(a, 0).
\]

Then
\[
S(a) = \begin{cases}
\begin{aligned}
(-1)^m12^{m+1} & \\
(-1)^m2^{m} & \end{aligned}
\end{cases},
\]

according as \(a\) is or is not a cube in \(\mathbb{GF}(q)\).

If \(a = c^3\), \(c \in \mathbb{GF}(q)\), then
\[
S(c^3, b) = \begin{cases}
\begin{aligned}
(-1)^m12^{m+1}e(u_0^3) & \\
0 & \end{aligned}
\end{cases},
\]

according as
\[
\sum_{j=0}^{m-1} (bc^{-1})^{2j} = 0
\]
is or is not satisfied; \( u_0 \) denotes any solution of \( u^4 + u = b^2 c^{-2} \).

If \( a \neq c^3 \), \( c \in \text{GF} (q) \), then

\[
S(a, b) = (-1)^m 2^m e(ax_0^3),
\]

where \( x_0 \) is the unique solution of \( a^2 x^4 + ax = b^2 \) given by (3.9).

4.

Let \( q = 2^n, n = 2m + 1 \). In this case the sum

\[
\sum_{x \in \text{GF}(q)} e(ax^3) = \sum_x e(ax) = 0 \quad (a \neq 0).
\]

Also, if \( a \neq 0 \), then \( a = c^3, c \in \text{GF}(q) \), so that

\[
\sum_x e(ax^3 + bx) = \sum_x e(c^3 x^3 + bx) = \sum_x e(c^3 + bc^{-1}x).
\]

Hence there is no loss in restricting the discussion to

(4.1) \[ S(1, b) = \sum_x e(x^3 + bx). \]

In particular put

(4.2) \[ S = S(1, 1) = \sum_x e(x^3 + x). \]

Then

(4.3) \[ S^2 = \sum_{x, y} e(x^3 + y^3 + x + y) \]

\[ = \sum_{x, y} e((x+y)^3 + y^3 + (x+y) + y) \]

\[ = \sum_x e(x^3 + x) \sum_y e(x^2 y + xy^2). \]

The inner sum is equal to

\[ \sum_y e((x^4 + x)y^2) = 0 \]

unless

(4.4) \[ x^4 + x = 0. \]

The four solutions of (4.4) constitute the GF (2^2). Since \( q = 2^{2m+1} \), the only solutions of (4.4) that lie in GF (q) are \( x = 0 \) and \( x = 1 \). Hence (4.3) gives

(4.5) \[ S^2 = 2q = 2^{2m+2}, \]
so that $S \neq 0$.

In (4.2) replace $x$ by $x + c^2$. We get

\[
S = \sum_x e((x + c^2)^3 + x + c^2)
\]

\[
= e(c^6 + c^2) \sum_x e(x^3 + c^2x^2 + c^4x + x)
\]

\[
= e(c^3 + c) \sum_x e(x^3 + (c^4 + c + 1)x)
\]

Thus

\[ S(1, c^4 + c + 1) = e(c^3 + c)S. \]

Let $b$ denote any number of GF $(q)$ such that $e(b) = -1$, that is, any number that satisfies

\[ b + b^2 + b^{22} + \ldots + b^{2^m} = 1. \]

Exactly half the numbers of GF $(q)$ satisfy (4.7). Then $b = a + 1$, where $e(a) = +1$, so that $a = c_1^2 + c_1$, $c_1 \in$ GF $(q)$. Since either $c_1$ or $c_1 + 1$ is equal to $c^2 + c$, we get $a = c^4 + c$, $c \in$ GF $(q)$. Hence $b = c^4 + c + 1$, that is, every solution of (4.7) is of this form and the corresponding sum $S(1, b)$ satisfies (4.6).

Next let $e(b) = +1$. Then

\[
S^2(1, b) = \sum_{x, y} e(x^3 + y^3 + bx + by)
\]

\[
= \sum_{x, y} e(x^3 + x^2y + xy^2 + bx)
\]

\[
= \sum_x e(x^3 + bx) \sum_y e(x^2y + xy^2)
\]

\[
= \sum_x e(x^3 + bx) \sum_y e((x^4 + x)y^2)
\]

\[
= q(1 + e(b + 1)) = 0.
\]

Thus

\[ S(1, b) = 0 \quad (e(b) = +1). \]

Hence, in view of (4.6), it will suffice to evaluate $S$. Indeed, by (4.5),

\[ S = \varepsilon \cdot 2^{m+1} \quad (\varepsilon = \pm 1). \]

To determine $\varepsilon$ let $N = N(q)$ denote the number of solutions $x, y \in$ GF $(q)$ of

\[ x^3 + x = y^2 + y; \]
also let \( N' = N'(q) \) denote the number of solutions \( x, y \in GF(q) \) of (4.10) such that \( x \) is not in any proper subfield of \( GF(q) \). If \( (x, y) \) is such a solution then

\[
(x^{2^j}, y^{2^j}) \quad (j = 0, 1, \ldots, 2m)
\]

are also such solutions and are all distinct. Hence we have

\[
(4.11) \quad N'(2^{2m+1}) \equiv 0 \pmod{2m+1}.
\]

Also clearly \( N'(2) = 4 \).

As for \( N(q) \), we have

\[
qN(q) = \sum_a \sum_{x, y} e(a(x^3 + x + y^2 + y))
\]

\[
= q^2 + \sum_{a \neq 0} \sum_x e(a(x^3 + x)) \sum_y e(a(y^2 + y)).
\]

The sum on the extreme right is equal to

\[
\sum_y e((a + a^2)y^2) = 0 \quad (a + a^2 \neq 0).
\]

Hence

\[
(4.12) \quad N(q) = q + S.
\]

It is clear from the definition of \( N(q) \) and \( N'(q) \) that

\[
N(2^{2m+1}) = \sum_{d \mid 2m+1} N'(2^d).
\]

Hence, by the Möbius inversion formula,

\[
(4.13) \quad N'(2^{2m+1}) = \sum_{d \mid 2m+1} \mu\left(\frac{2m+1}{d}\right)N(2^d).
\]

By (4.9) and (4.12) we have

\[
(4.14) \quad N(2^n) = 2^n + \varepsilon_n \cdot 2^{(n+1)/2} \quad (\varepsilon_n = \pm 1);
\]

the fuller notation \( \varepsilon_n \) is needed for what follows.

To begin with we take \( 2m+1 = p \), where \( p \) is prime. Then (4.13) becomes

\[
N'(2^p) = N(2^p) - N(2)
\]

\[
= 2^p + \varepsilon_p \cdot 2^{(p+1)/2} - 4.
\]

Thus, by (4.11),

\[
\varepsilon_p \cdot 2^{(p-1)/2} \equiv 1 \pmod{p},
\]

so that \( \varepsilon_p = (2/p) \), the Legendre symbol.

Next let \( 2m+1 = p' \). Then
\[ N'(2^{p^r}) = 2^{p^r} + e_{p^r} \cdot 2^{(p^r + 1)/2} - 2^{p^r - 1} - e_{p^r - 1} \cdot 2^{(p^r - 1 + 1)/2}, \]

so that, by (4.11),
\[ e_{p^r} \cdot 2^{(p^r - 1)/2} \equiv e_{p^r - 1} \cdot 2^{(p^r - 1 - 1)/2} \pmod{p}. \]

It follows that
\[ (4.15) \quad e_{p^r} = \left( \frac{2}{p^r} \right) = \left( \frac{2}{p} \right)^r. \]

We shall show that generally
\[ (4.16) \quad e_{2m + 1} = \left( \frac{2}{2m + 1} \right), \]
the Jacobi symbol. The following lemma will be used.

**Lemma.** We have
\[ (4.17) \quad \sum_{rs = 2m + 1} \mu(r) \left( \frac{2}{s} \right) 2^{(s-1)/2} \equiv 0 \pmod{M}, \]
where \( M \) denotes the product of the distinct prime divisors of \( 2m + 1 \).

**Proof.** Let \( f(2m + 1) \) denote the left member of (4.17). It is easily seen that \( f(2m + 1) \) is a factorable function of \( 2m + 1 \). For \( 2m + 1 \) equal to a prime power \( p^r \) we have
\[ f(p^r) = \left( \frac{2}{p^r} \right) 2^{(p^r - 1)/2} - \left( \frac{2}{p^{r-1}} \right) 2^{(p^r - 1 - 1)/2} \]
\[ = \left( \frac{2}{p^r} \right) \left( \frac{2}{p} \right)^r - \left( \frac{2}{p^{r-1}} \right) \left( \frac{2}{p} \right)^{r-1} \equiv 0 \pmod{p}. \]

This completes the proof of the lemma.

We shall now prove (4.16). By (4.13) and (4.14),
\[ (4.18) \quad N'(2^{2m+1}) = \sum_{rs = 2m + 1} \mu(r) 2^s + \sum_{rs = 2m + 1} \mu(r) e_s \cdot 2^{(s+1)/2}. \]

It is well known that
\[ \sum_{rs = 2m + 1} \mu(r) 2^s \equiv 0 \pmod{2m + 1}. \]

Hence (4.18) implies
\[ (4.19) \quad \sum_{rs = 2m + 1} \mu(r) e_s \cdot 2^{(s+1)/2} \equiv 0 \pmod{M}. \]
Assume that

\[ (4.20) \quad \varepsilon_s = \left(\frac{2}{s}\right) \]

for all proper divisors of \(2m+1\). Then (4.19) becomes

\[
\sum_{\substack{rs = 2m+1 \\ s < 2m+1}} \mu(r) \left(\frac{2}{s}\right) 2^{(s+1)/2} + \varepsilon_{2m+1} \cdot 2^{m+1} \equiv 0 \pmod{M}.
\]

By (4.17),

\[
\sum_{\substack{rs = 2m+1 \\ s < 2m+1}} \mu(r) \left(\frac{2}{s}\right) 2^{(s+1)/2} + \left(\frac{2}{2m+1}\right) 2^{m+1} \equiv 0 \pmod{M}
\]

and therefore

\[
\varepsilon_{2m+1} = \left(\frac{2}{2m+1}\right).
\]

Thus (4.9) becomes

\[ (4.21) \quad S = \left(\frac{2}{2m+1}\right) 2^{m+1} \quad (q = 2^{2m+1}) \]

and (by 4.6),

\[ (4.22) \quad S(1, c^4 + c + 1) = e(c^3 + c) \left(\frac{2}{2m+1}\right) 2^{m+1} . \]

We may now state

**Theorem 2.** Let \( q = 2^{2m+1} \), \( b \neq 0 \),

\[
S(1, b) = \sum_{x \in \mathbb{F}_q} e(x^3 + bx). 
\]

Then

\[
S(1, 1) = \left(\frac{2}{2m+1}\right) 2^{m+1},
\]

where \( (2/2m+1) \) is the Jacobi symbol. If \( e(b) = -1 \), put \( b = c^4 + c + 1 \); then

\[
S(1, b) = e(c^3 + c) \left(\frac{2}{2m+1}\right) 2^{m+1}.
\]

Finally

\[
S(1, b) = 0 \quad (e(b) = +1) .
\]
REFERENCES


DUKE UNIVERSITY
DURHAM, N.C. 27706
U.S.A.