MATH SCAND. 42 (1978), 39–48

A NOTE ON EXPONENTIAL SUMS

L. CARLITZ

1.

Let $F=\mathrm{GF}(q)$ denote the finite field of odd characteristic p, where $q=p^n$, $n\geqq 1$. For $a\in F$, put

$$t(a) = a+a^p+a^{p^2}+\ldots+a^{p^{n-1}}$$

and

$$e(a) = e^{2\pi i t(a)/p}.$$

We define the exponential sums

$$S(a,b) = \sum_{x\in F} e(ax^3+bx) \tag{1.1}$$

and

$$T(a,b) = \sum_{x\in F} e(ax^6+bx^2), \tag{1.2}$$

where $a,b\in F$.

The object of this note is to prove a simple relation connecting $S(a,b)$ and $T(a,b)$. Assume $p>3$, $a\neq 0$. Then we show that

$$\psi(3a)T(a,b)G = S^2(4a,b)+\psi(3a)S(a,b)G-q, \tag{1.3}$$

where $\psi(a)=+1,-1,0$ according as a is a non-zero square, a non-square or the zero element of F and G is the Gauss sum defined by

$$G(a) = \sum_{x\in F} \psi(x)e(ax), \qquad G = G(1). \tag{1.4}$$

Since $|G|=q^{\frac{1}{2}}$, it follows at once from (1.3) that the two estimates

$$S(a,b) = O(q^{\frac{1}{2}}), \qquad T(a,b) = O(q^{\frac{1}{2}})$$

are equivalent.

The method used in proving (1.3) applies as well to the sum

$$U(a,b,c) = \sum_{x,y\in F} e\{a(x^3+y^3)+b(x^2y+xy^2)+c(x+y)\}. \tag{1.5}$$

Received April 29, 1977.

We show that

$$U(a,3a,c) = qS(a,c)\,, \tag{1.6}$$

$$U(a,-a,c) = (1+\psi(-ac))q \tag{1.7}$$

and

$$U(a,b,c)-q = \psi(3(a+b)(3a-b))(S^2(a+b,c)-q) \quad ((a+b)(3a-b)\neq 0)\,. \tag{1.8}$$

In particular, if $\psi(3(a+b)(3a-b))=1$ then

$$U(a,b,c) = S^2(a+b,c)\,. \tag{1.9}$$

For the evaluation of $S(a,b)$, $T(a,b)$, $U(a,b,c)$ when $p=3$ or 2, see sections 4 and 5 below.

2.

We recall that

$$e(a+b) = e(a)e(b)\,, \tag{2.1}$$

$$\sum_{x\in F} e(ax) = \begin{cases} q & (a=0) \\ 0 & (a\neq 0)\,, \end{cases} \tag{2.2}$$

$$\sum_{x\in F} \psi(x) = 0 \tag{2.3}$$

and

$$G(a) = \psi(a)G\,. \tag{2.4}$$

Also it follows from the definition of $\psi(a)$ that the number of solutions $x, y \in F$ of

$$x+y = u, \quad xy = v$$

is equal to $1+\psi(u^2-4v)$.

We have, by (1.1) and (2.1),

$$\begin{aligned} S^2(a,b) &= \sum_{x,y\in F} e(a(x^3+y^3)+b(x+y)) \\ &= \sum_{x,y\in F} e(a(x+y)^3-3axy(x+y)+b(x+y))\,. \end{aligned}$$

Put $u=x+y$, $v=xy$, so that

$$\begin{aligned} S^2(a,b) &= \sum_{u,v\in F} (1+\psi(u^2-4v))e(au^3+bu-3auv) \\ &= S_1+S_2\,, \end{aligned}$$

where

$$S_1 = \sum_{u,v} e(au^3+bu-3auv)\,, \tag{2.5}$$

$$S_2 = \sum_{u,v} \psi(u^2-4v)e(au^3+bu-3auv)\,. \tag{2.6}$$

Thus, by (2.1) and (2.2),

$$\begin{aligned} S_1 &= \left\{\sum_{u=0}\sum_{v}+\sum_{u\neq 0}\sum_{v}\right\}e(au^3+bu-3auv) \\ &= q+\sum_{u\neq 0} e(au^3+bu)\sum_{v} e(-auv)\,, \end{aligned}$$

so that

$$S_1 = q\,. \tag{2.7}$$

As for S_2, we have

$$S_2 = \left\{\sum_{u=0}\sum_{v}+\sum_{u\neq 0}\sum_{v}\right\}\psi(u^2-4v)e(au^3+bu-3auv)\,.$$

It follows from (2.3) that

$$\sum_{u=0}\sum_{v}\psi(u^2-4v)e(au^3+bu-3auv) = \sum_{v}\psi(-4v) = 0\,.$$

Thus

$$\begin{aligned} S_2 &= \sum_{u\neq 0}\sum_{v}\psi(u^2+4v)e(au^3+bu+3auv) \\ &= \sum_{u\neq 0}\sum_{v}\psi(4v)e\{au^3+bu+3au(v-\tfrac{1}{4}u^2)\} \\ &= \sum_{u\neq 0}\sum_{v}\psi(v)e(\tfrac{1}{4}au^3+bu+3auv) \\ &= \sum_{u\neq 0} e(\tfrac{1}{4}au^3+bu)\sum_{v}\psi(v)e(3auv)\,. \end{aligned}$$

Hence, by (1.4) and (2.4),

$$S_2 = \psi(3a)G\sum_{u}\psi(u)e(\tfrac{1}{4}au^3+bu)\,. \tag{2.8}$$

Thus, by (2.5), (2.6), (2.7) and (2.8),

$$S^2(4a,b) = q+\psi(3a)G\sum_{u}\psi(u)e(au^3+bu)\,. \tag{2.9}$$

In the next place, by (1.2),

$$T(a,b) = \sum_x e(ax^6+bx^2) \tag{2.10}$$

$$= \sum_u (1+\psi(u))e(au^3+bu)$$

$$= S(a,b)+\sum_u \psi(u)e(au^3+bu)\,.$$

Thus (2.9) becomes

$$S^2(4a,b) = q+\psi(3a)G\cdot\{T(a,b)-S(a,b)\}\,.$$

This evidently completes the proof of (1.3).

3.

The sum

$$U(a,b,c) = \sum_{x,\,y\in F} e\{a(x^3+y^3)+b(x^2y+xy^2)+c(x+y)\}$$

$$= \sum_{u,\,v\in F} \{1+\psi(u^2-4v)\}e\{a(u^3-3uv)+buv+cu\}$$

$$= U_1+U_2\,,$$

where

$$U_1 = \sum_{u,\,v} e\{au^3-(3a-b)uv+cu\}$$

$$U_2 = \sum_{u,\,v} \psi(u^2-4v)e\{au^3-(3a-b)uv+cu\}\,.$$

We have

$$U_1 = \sum_u e(au^3+cu)\sum_v e(-(3a-b)uv)\,.$$

Since

$$\sum_v e(-(3a-b)uv) = \begin{cases} q & ((3a-b)u=0) \\ 0 & (\text{otherwise})\,, \end{cases}$$

it follows that

$$U_1 = q\sum_u e(au^3+cu) = qS(a,c) \qquad (b=3a) \tag{3.1}$$

while

$$U_1 = q \qquad (b\neq 3a)\,. \tag{3.2}$$

As for U_2, we have

$$\begin{aligned} U_2 &= \sum_{u,v} \psi(u^2+4v)e\{au^3+(3a-b)uv+cu\} \\ &= \sum_{u,v} \psi(4v)e\{au^3+(3a-b)u(v-\tfrac{1}{4}u^2)+cu\} \\ &= \sum_{u,v} \psi(4v)e\{\tfrac{1}{4}(a+b)u^3+(3a-b)uv+cu\} \\ &= \sum_{u} e\{\tfrac{1}{4}(a+b)u^3+cu\} \sum_{v} \psi(v)e((3a-b)uv) \\ &= \psi(3a-b)G \sum_{u} \psi(u)e\{\tfrac{1}{4}(a+b)u^3+cu\} . \end{aligned}$$

Hence, by (2.8),

$$U_2 = \psi(3(a+b)(3a-b))(S^2(a+b,c)-q) \qquad (a+b\neq 0) . \tag{3.3}$$

Finally, by (3.1), (3.2) and (3.3),

$$U(a,b,c) = qS(a,c) \qquad (b=3a) \tag{3.4}$$

but

$$U(a,b,c)-q = \psi(3(a+b)(3a-b))(S^2(a+b,c)-q)((a+b)(3a-b)\neq 0) . \tag{3.5}$$

If $a+b=0$ we have from the proof of (3.3),

$$\begin{aligned} U_2 &= \sum_{u,v} \psi(v)e(auv+cu) \\ &= \psi(a)G \sum_{u} \psi(u)e(cu) \\ &= \psi(ac)G^2 . \end{aligned}$$

Since $G^2=\psi(-1)q$, it follows that

$$U_2 = \psi(-ac)q . \tag{3.6}$$

Hence, by (3.2) and (3.6), we have

$$U(a,-a,c) = (1+\psi(-ac))q . \tag{3.7}$$

4.

If $p=3$ then $e(a)=e(a^3)$. Thus

$$S(a^3,b) = \sum_{x\in F} e(a^3x^3+bx) = \sum_{x\in F} e((a+b)x) .$$

Hence, by (2.2),

$$S(a^3,b) = \begin{cases} q & (a+b=0) \\ 0 & (a+b\neq 0)\,. \end{cases} \tag{4.1}$$

As for $T(a,b)$, we have

$$T(a^3,b) = \sum_{x\in F} e(a^3x^6bx^2) = \sum_{x\in F} e((a+b)x^2)\,.$$

Thus, by (2.4),

$$T(a^3,b) = \begin{cases} q & (a+b=0) \\ \psi(a+b)G & (a+b\neq 0)\,. \end{cases} \tag{4.2}$$

Since every element of GF (3^n) is a cube there is no loss in generality in considering $S(a^3,b)$, $T(a^3,b)$.

In the next place

$$\begin{aligned} U(a^3,4b^3,c) &= \sum_{x,y\in F} e\{a^3(x^3+y^3)+4b^3(x^2y+xy)+c(x+y)\} \\ &= \sum_{x,y\in F} e\{(a+c)(x+y)+4b^3(x+y)xy\} \\ &= \sum_{u,v\in F} \{1+\psi(u^2-4v)\}e((a+c)u+4b^3uv) \\ &= U_1+U_2\,, \end{aligned} \tag{4.3}$$

where

$$U_1 = \sum_{u,v\in F} e((a+c)u+4b^3uv) \qquad U_2 = \sum_{u,v\in F} \psi(u^2-4v)e((a+c)u+4b^3uv)\,.$$

We have

$$U_1 = \sum_{u\in F} e((a+c)u) \sum_{v\in F} e(4b^3uv)\,.$$

Assume $b\neq 0$, so that the inner sum vanishes unless $u=0$. It follows that

$$U_1 = q\,. \tag{4.4}$$

As for U_2, we have

$$\begin{aligned} U_2 &= \sum_{u,v\in F} \psi(4v)e\{(a+c)u-4b^3u(v-\tfrac{1}{4}u^2)\} \\ &= \sum_{u,v\in F} \psi(v)e\{(a+b+c)u-4b^3uv)\} \\ &= \sum_{u\in F} e((a+b+c)u) \sum_{v\in F} \psi(v)e(-4b^3uv) \end{aligned}$$

$$= G\psi(-b) \sum_{u \in F} \psi(u) e((a+b+c)u)$$

$$= G\psi(-b) \cdot \psi(a+b+c) G .$$

Since $G^2 = \psi(-1)q$, we get

$$U_2 = \psi((a+b+c)b)q . \tag{4.5}$$

Therefore, by (4.3), (4.4) and (4.5),

$$U(a^3, 4b^3, c) = (1+\psi((a+b+c)b))q \qquad (b \neq 0) . \tag{4.6}$$

5.

The case $p=2$ is somewhat more interesting. As above

$$S^2(a,b) = \sum_{x,y \in F} e(a(x^3+y^3)+b(x+y)) .$$

We again put

$$x+y = u, \quad xy = v . \tag{5.1}$$

For fixed u, v the number of solutions of (5.1) is equal to the number of solutions of

$$x^2+ux = v . \tag{5.2}$$

For $u=0$ and arbitrary v, (5.2) *has a single solution. For* $u \neq 0$, put $x=zu$. Then (5.2) becomes

$$z^2+z = u^{-2}v . \tag{5.3}$$

Equation (5.3) is solvable if and only if [2, p. 29] $t(u^{-2}v)=0$. Thus the number of solutions of (5.3) is equal to

$$1+e(u^{-2}v) \qquad (u \neq 0) . \tag{5.4}$$

Therefore the number of solutions of (5.1) is equal to

$$N(u,v) = \begin{cases} 1 & (u=0) \\ 1+e(u^{-2}v) & (u \neq 0) . \end{cases} \tag{5.5}$$

We now get

$$S^2(a,b) = \sum_{u,v \in F} N(u,v) e(a(u^3+uv)+bu) \tag{5.6}$$

$$= \sum_{v \in F} N(0,v) + \sum_{\substack{u,v \in F \\ u \neq 0}} N(u,v) e(a(u^3+uv)+bu)$$

$$= q + \sum_{\substack{u,v \in F \\ u \neq 0}} (1 + e(u^{-2}v))e(a(u^3 + uv) + bu)$$

$$= q + S_1 + S_2 ,$$

where

$$S_1 = \sum_{\substack{u,v \in F \\ u \neq 0}} e(au^3 + auv + bu)$$

$$S_2 = \sum_{\substack{u,v \in F \\ u \neq 0}} e(au^3 + u^{-2}v + auv + bu) .$$

Assume $a \neq 0$. It follows from (2.2) that

$$S_1 = 0 . \tag{5.7}$$

As for S_2, we have

$$S_2 = \sum_{u \neq 0} e(au^3 + bu) \sum_v ((u^{-2} + au)v) .$$

The inner sum vanishes unless $au^3 = 1$.

There are several possibilities. Assume first that n is odd, where $q = 2^n$. Then the equation $au^3 = 1$ has a unique solution $u_0 \neq 0$. Since

$$e(1 + bu_0) = e(1)e(bu_0) = (-1)^n e(bu_0) = -e(bu_0) ,$$

it follows that

$$S_2 = -e(bu_0)q \qquad (q = 2^n,\ n \text{ odd}) . \tag{5.8}$$

On the other hand, if n is even, the equation $au^3 = 1$ may or may not be solvable. If the equation is not solvable then clearly $S_2 = 0$. If it is solvable it has three distinct solutions, say u_0, u_1, u_2 and we get

$$S_2 = (e(bu_0) + e(bu_1) + e(bu_2))q \tag{5.8}'$$

Therefore, by (5.6), (5.7), (5.8), (5.8)', we have

$$S^2(a,b) = (1 - e(bu_0))q \qquad (q = 2^n,\ n \text{ odd}) , \tag{5.9}$$

while, for n even,

$$(5.9)'\ S^2(a,b) = \begin{cases} q & (au^3 = 1 \text{ not solvable}) \\ ((1 + e(bu_0) + e(bu_1) + e(bu_2))q , \end{cases}$$

where u_0, u_1, u_2 are the three solutions of $au^3 = 1$. It is assumed throughout that $a \neq 0$. Also it can be verified that the coefficient of q in the final formula is equal to either 0 or 4. Thus $S(a,b)$ is evaluated except for sign.

The sum $T(a,b)$ evidently satisfies

$$T(a^2,b^2) = S(a,b)\,. \tag{5.10}$$

Finally

$$\begin{aligned} U(a,b,c) &= \sum_{x,\,y\in F} e\{a(x^3+y^3)+b(x+y)xy+c(x+y)\} \\ &= \sum_{u,\,v\in F} N(u,v)e(a(u^3+uv)+buv+cu) \\ &= q+U_1+U_2\,, \end{aligned} \tag{5.11}$$

where

$$U_1 = \sum_{\substack{u,\,v\\ u\neq 0}} e(a(u^3+uv)+buv+cu)$$

$$U_2 = \sum_{\substack{u,\,v\\ u\neq 0}} e(a(u^3+uv)+u^{-2}v+buv+cu)\,.$$

Then

$$U_1 = \sum_{u\neq 0} e(au^3+cu)\sum_{v} e'((a+b)uv)\,,$$

which yields

$$U_1 = \begin{cases} (-1+S(a,c))q & (a=b) \\ 0 & (a\neq b)\,. \end{cases} \tag{5.12}$$

Similarly

$$U_2 = \sum_{u\neq 0} e(au^3+cu)\sum_{v} e(((a+b)u+u^{-2})v)\,.$$

Since

$$\sum_{v} e(((a+b)u+u^{-2})v) = \begin{cases} q & ((a+b)u^3=1) \\ 0 & ((a+b)u^3\neq 1)\,, \end{cases}$$

there are again several possibilities.

It is evident, to begin with, that

$$U_2 = 0 \quad (a=b)\,. \tag{5.13}$$

Assume $a\neq b$. Then if $q=2^n$, n odd, we have

$$U_2 = e(a(a+b)^{-1}+cu_0)q\,, \tag{5.14}$$

where u_0 is the unique solution of $(a+b)u^3=1$. For n even we get

$$U_2 = \begin{cases} 0 & ((a+b)u^3 = 1 \text{ not solvable}) \\ e(a(a+b)^{-1})(e(cu_0)+e(cu_1)+e(cu_2))q\,, \end{cases} \tag{5.15}$$

where u_0, u_1, u_2 are the three solutions of $(a+b)u^3 = 1$. Therefore by (5.11),..., (5.15),

$$U(a,b,c) = S(a,c)q \qquad (a=b); \tag{5.16}$$

$$U(a,b,c) = (1+e(a(a+b)^{-1}+cu_0))q \qquad (n \text{ odd}, \ (a+b)u_0^3 = 1); \tag{5.17}$$

$$U(a,b,c) = \begin{cases} q & ((a+b)u^3 = 1 \text{ not solvable}) \\ (1+e(a(a+b)^{-1})(e(cu_0)+e(cu_1)+e(cu_2)))q \end{cases} \tag{5.18}$$

where n is even and u_0, u_1, u_2 are the three solutions of $(a+b)u^3 = 1$.

We remark that, for $q = 2^n$, the sums $S(a,b)$, $T(a,b)$, $U(a,b,c)$ are all rational integers.

For a similar evaluation of the sum

$$\sum_{x \neq 0} \sum_{y \neq 0} e(x+y+a(xy)^{-1}),$$

see [1].

REFERENCES

1. L. Carlitz, *A note on exponential sums*, Pacific J. Math. 30 (1969), 35–37.
2. L. E. Dickson, *Linear Groups with an Exposition of the Galois Field Theory*, Dover, New York, 1958.

DEPARTMENT OF MATHEMATICS
DUKE UNIVERSITY
DURHAM, NORTH CAROLINA 27706
U.S.A.