PACIFIC JOURNAL OF MATHEMATICS
Vol. 30, No. 1, 1969

A NOTE ON EXPONENTIAL SUMS

L. CARLITZ

Put $S(a) = \sum_{x,y\neq 0} e(x + y + ax^1y^1)$, **where** $xx^1 = yy^1 = 1$, $e(x) = x + x^2 + \cdots + x^{2^{n-1}}$ **and the summation is over all nonzero** x, y **in the finite field** $GF(q)$, $q = 2^n$. **Then it is shown that** $S(a) = 0(q)$ **for all** $a \in GF(a)$.

Let p be a prime and put

$$S_2(a) = \sum_{x,y=1}^{p-1} e(x + y + ax'y') ,$$

where $e(x) = e^{2\pi ix/p}$ and $xx' \equiv yy' \equiv 1 \pmod p$. For $a = 0$ it is evident that $S(0) = 1$. Mordell [3] has conjectured that

$$(1) \qquad S_2(a) = 0(p)$$

for all a. The writer [1] has proved that

$$S_2(a) = 0(p^{5/4})$$

for all a.

For the finite field $GF(q)$, $q = p^n$, we may define

$$S_2(a) = \sum_{x,y\neq 0} e(x + y + ax'y') ,$$

where $a \in GF(q)$,

$$(2) \qquad e(x) = e^{2\pi it(x)/p},\ t(x) = x + x^p + \cdots + x^{p^{n-1}} ,$$

$xx' = yy' = 1$, and the summation is over all nonzero $x, y \in GF(q)$. We may conjecture that

$$(3) \qquad S_2(a) = 0(q)$$

for all $a \in GF(q)$.

In this note we show that (3) holds for $q = 2^n$. Indeed if

$$S_1(a) = \sum_{x\neq 0} e(x + ax') ,$$

we show that, for $a \neq 0$,

$$(4) \qquad S_1^2(a) = q + S_2(a) \qquad (q = 2^n) .$$

Since [2], [4]

$$(5) \qquad |S_1(a)| \leqq 2q^{1/2} ,$$

it is clear that (3) follows from (4) and (5). Indeed a little more can be said. Since, for $q = 2^n$, $e(a) = \pm 1$, it follows that both $S_1(a)$ and $S_2(a)$ are rational integers and in fact nonzero. Hence (4) and (5) give

$$-q < S_2(a) \leqq 3q \; . \tag{6}$$

2. To prove (4), we take

$$\begin{aligned} S_1^2(a) &= \sum_{x,y\neq 0} e[x + y + a(x' + y')] \\ &= \sum_{x,y\neq 0} e[x + y + a(x + y)x'y'] \; . \end{aligned}$$

If we put

$$u = x + y,\, v = xy \tag{7}$$

then

$$S_1^2(a) = \sum_{\substack{u,v \\ v\neq 0}} e(u + auv')N(u, v) \; , \tag{8}$$

where $N(u, v)$ denotes the number of solutions x, y of (7); since $v \neq 0$, x and y are automatically $\neq 0$.

For $u = 0$, (7) reduces to $x^2 = v$, so that $N(0, v) = 1$ for all v. For $u \neq 0$, (7) is equivalent to

$$x^2 + ux = v \; . \tag{9}$$

The condition for solvability of (9) is $t(u^{-2}v) = 0$, where $t(x)$ is defined by (2). Hence the number of solutions of (9) is equal to $1 + e(u^{-2}v)$, so that

$$N(u, v) = 1 + e(u'^2 v) \qquad (uv \neq 0) \; . \tag{10}$$

Substituting from (10) in (8), we get

$$\begin{aligned} S_1^{(2)}(a) &= \sum_{v\neq 0} N(0, 1) + \sum_{u,v\neq 0} e(u + auv')N(u, v) \\ &= \sum_{v\neq 0} 1 + \sum_{u,v\neq 0} e(u + auv')\{1 + e(u'^2 v)\} \\ &= q - 1 + \sum_{u,v\neq 0} e(u+auv') + \sum_{u,v\neq 0} e(u + u'^2 v + auv') \; . \end{aligned}$$

Since

$$\sum_{u\neq 0} e(au) = -1 \qquad (a \neq 0) \; ,$$

it follows, for $a \neq 0$, that

$$S_1^2(a) = q + \sum_{u,v\neq 0} e(u + u'^2 v + auv') \; .$$

Replacing v by $u^2 v$, this becomes

$$S_1^2(a) = q + \sum_{u, v \neq 0} e(u + v + au'v')$$
$$= q + S_2(a) ,$$

so that we have proved (4).

3. We may define

$$S_3(a) = \sum_{x, y, z \neq 0} e(x + y + z + ax'y'z') .$$

The writer has been unable to find a relation like (4) involving $S_3(a)$.

References

1. L. Carlitz, *A note on multiple exponential sums*, Pacific J. Math. **15** (1965), 757-765.
2. L. Carlitz and S. Uchiyama, *Bounds for exponential sums*, Duke Math. J. **24** (1957), 37-41.
3. L. J. Mordell, *On a special polynomial congruence and exponential sum*, Calcutta Mathematical Society Golden Jubilee Commemoration Volume, 1958/59, part 1, 29-32.
4. A. Weil, *Some exponential sums*, Proc. Nat. Acad. Sci. **34** (1949), 204-207.

Received June 17, 1968. Supported in part by NSF grant GP-5174.

DUKE UNIVERSITY
DURHAM, NORTH CAROLINA