

Pacific Journal of Mathematics

A NOTE ON EXPONENTIAL SUMS

L. CARLITZ

A NOTE ON EXPONENTIAL SUMS

L. CARLITZ

Put $S(a) = \sum_{x, y \neq 0} e(x + y + ax'y')$, where $xx' = yy' = 1$, $e(x) = x + x^2 + \cdots + x^{2^n-1}$ and the summation is over all non-zero 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

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

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 $a \in GF(q)$,

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

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

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

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 $a \neq 0$,

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

Since [2], [4]

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

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

$$(6) \quad -q < S_2(a) \leq 3q .$$

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

$$(7) \quad u = x + y, v = xy$$

then

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

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

$$(9) \quad x^2 + ux = v .$$

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

$$(10) \quad N(u, v) = 1 + e(u'^2v) \quad (uv \neq 0) .$$

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

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

Since

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

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

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

Replacing v by u^2v , this becomes

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

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 I, 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

PACIFIC JOURNAL OF MATHEMATICS

EDITORS

H. ROYDEN
Stanford University
Stanford, California

J. DUGUNDJI
Department of Mathematics
University of Southern California
Los Angeles, California 90007

RICHARD PIERCE
University of Washington
Seattle, Washington 98105

BASIL GORDON
University of California
Los Angeles, California 90024

ASSOCIATE EDITORS

E. F. BECKENBACH

B. H. NEUMANN

F. WOLF

K. YOSHIDA

SUPPORTING INSTITUTIONS

UNIVERSITY OF BRITISH COLUMBIA
CALIFORNIA INSTITUTE OF TECHNOLOGY
UNIVERSITY OF CALIFORNIA
MONTANA STATE UNIVERSITY
UNIVERSITY OF NEVADA
NEW MEXICO STATE UNIVERSITY
OREGON STATE UNIVERSITY
UNIVERSITY OF OREGON
OSAKA UNIVERSITY
UNIVERSITY OF SOUTHERN CALIFORNIA

STANFORD UNIVERSITY
UNIVERSITY OF TOKYO
UNIVERSITY OF UTAH
WASHINGTON STATE UNIVERSITY
UNIVERSITY OF WASHINGTON
* * *
AMERICAN MATHEMATICAL SOCIETY
CHEVRON RESEARCH CORPORATION
TRW SYSTEMS
NAVAL WEAPONS CENTER

Pacific Journal of Mathematics

Vol. 30, No. 1

September, 1969

William Wells Adams, <i>Simultaneous diophantine approximations and cubic irrationals</i>	1
Heinz Bauer and Herbert Stanley Bear, Jr., <i>The part metric in convex sets</i>	15
L. Carlitz, <i>A note on exponential sums</i>	35
Vasily Cateforis, <i>On regular self-injective rings</i>	39
Franz Harpain and Maurice Sion, <i>A representation theorem for measures on infinite dimensional spaces</i>	47
Richard Earl Hodel, <i>Sum theorems for topological spaces</i>	59
Carl Groos Jockusch, Jr. and Thomas Graham McLaughlin, <i>Countable retracing functions and Π_2^0 predicates</i>	67
Bjarni Jónsson and George Stephen Monk, <i>Representations of primary Arguesian lattices</i>	95
Virginia E. Walsh Knight, <i>A continuous partial order for Peano continua</i>	141
Kjeld Laursen, <i>Ideal structure in generalized group algebras</i>	155
G. S. Monk, <i>Desargues' law and the representation of primary lattices</i>	175
Hussain Sayid Nur, <i>Singular perturbation of linear partial differential equation with constant coefficients</i>	187
Richard Paul Osborne and J. L. Stern, <i>Covering manifolds with cells</i>	201
Keith Lowell Phillips and Mitchell Herbert Taibleson, <i>Singular integrals in several variables over a local field</i>	209
James Reaves Smith, <i>Local domains with topologically T-nilpotent radical</i>	233
Donald Platte Squier, <i>Elliptic differential equations with discontinuous coefficients</i>	247
Tae-il Suh, <i>Algebras formed by the Zorn vector matrix</i>	255
Earl J. Taft, <i>Ideals in admissible algebras</i>	259
Jun Tomiyama, <i>On the tensor products of von Neumann algebras</i>	263
David Bertram Wales, <i>Uniqueness of the graph of a rank three group</i>	271
Charles Robert Warner and Robert James Whitley, <i>A characterization of regular maximal ideals</i>	277