

Pacific Journal of Mathematics

A NOTE ON MULTIPLE EXPONENTIAL SUMS

L. CARLITZ

A NOTE ON MULTIPLE EXPONENTIAL SUMS

L. CARLITZ

Put

$$S(c) = \sum_{x,y=1}^{p-1} e(x + y + cx'y'),$$

Where $e(x) = e^{2\pi i x/p}$ and $xx' \equiv yy' \equiv 1 \pmod{p}$, Mordell has conjectured that $S(c) = O(p)$. The writer shows first, by an elementary argument that $S(c) = O(p^{3/2})$. Next he proves, using a theorem of Lang and Weil that $S(c) = O(p^{11/8})$. Finally he proves that $S(c) = O(p^{5/4})$; the proof makes use of the estimate

$$\sum_{x=0}^{p-1} \phi(f(x)) = O(p^{1/2}),$$

where $\phi(a)$ is the Legendre symbol and $f(x)$ is a polynomial of the fourth degree.

If we put

$$K(a, b) = \sum_{x=1}^{p-1} e(ax + bx'),$$

where $ab \not\equiv 0 \pmod{p}$, it is known that

$$(2) \quad |K(a, b)| \leq 2p^{1/2}.$$

For proof of (2) see [1], [4].

Since

$$\begin{aligned} S &= \sum_{x=1}^{p-1} e(ax) \sum_{y=1}^{p-1} e(by + cx'y') \\ &= \sum_{x=1}^{p-1} e(ax) K(b, cx'), \end{aligned}$$

it follows that

$$|S| \leq \sum_{x=1}^{p-1} |K(b, cx')| \leq 2(p-1)p^{1/2}$$

by (2). Thus, assuming (2), we get

$$(3) \quad S = O(p^{3/2}).$$

However it is not difficult to prove (3) directly without making use of (2). Put

Received July 28, 1964, and in revised form September 23, 1964, Supported in part by NSF Grant GP-1593.

$$(4) \quad S(c) = \sum_{x,y=1}^{p-1} e(x + y + cx'y').$$

There is evidently no loss in generality in taking $a = b = 1$. Then we have

$$\begin{aligned} \sum_{c=0}^{p-1} |S(c)|^2 &= \sum_{c=0}^{p-1} \sum_{x,y=1}^{p-1} \sum_{u,v=1}^{p-1} e\{x + y - uv + c(x'y' - u'v')\} \\ &= p \sum_{xy \equiv uv \pmod{p}} e(x + y - u - v). \end{aligned}$$

But

$$\begin{aligned} \sum_{xy \equiv uv \pmod{p}} e(x + y - u - v) &= \sum_{x,y,u=1}^{p-1} e(x + y - u - xyu') \\ &= \sum_{y,u=1}^{p-1} e(y - u) \sum_{x=1}^{p-1} e\{x(1 - yu')\} \\ &= - \sum_{y,u=1}^{p-1} e(y - u) + \sum_{y,u=1}^{p-1} e(y - u) \sum_{x=0}^{p-1} e\{x(1 - yu')\} \\ &= -1 + p \sum_{y=1}^{p-1} 1 = p^2 - p - 1, \end{aligned}$$

so that

$$(5) \quad \sum_{c=0}^{p-1} |S(c)|^2 = p^3 - p^2 - p.$$

It follows at once from (5) that

$$(6) \quad |S(c)| < p^{3/2},$$

so that we have proved (3).

2. Generalizing (4) we define

$$(7) \quad S_n(c) = \sum_{x_1, \dots, x_n=1}^{p-1} e(x_1 + \dots + x_n + cx'_1 \dots x'_n).$$

We shall show that

$$(8) \quad S_n(c) = O(p^{1/2(n+1)}).$$

Exactly as above we have

$$(9) \quad \sum_c |S_n(c)|^2 = p \sum_{x_1, \dots, x_n} \sum_{y_1, \dots, y_n} e(x_1 + \dots + x_n - y_1 - \dots - y_n),$$

where the summation is over all x_j, y_j such that

$$x_1 x_2 \dots x_n \equiv y_1 y_2 \dots y_n, \quad x_j \not\equiv 0, \quad y_j \not\equiv 0 \pmod{p}.$$

Let T_n denote the sum on the right of (9). Then we have

$$\begin{aligned}
 T_n &= \sum e(x_1 + \dots + x_n - y_1 - \dots - y_{n-1} - x_1 \dots x_n y'_1 \dots y'_{n-1}) \\
 &= \sum_{\substack{x_1, \dots, x_{n-1} \\ y_1, \dots, y_{n-1}}} e(x_1 + \dots + x_{n-1} - y_1 - \dots - y_{n-1}) \\
 &\quad \cdot \sum_x e[(1 - x_1 \dots x_{n-1} y'_1 \dots y'_{n-1})x] .
 \end{aligned}$$

The inner sum is equal to

$$\begin{cases} p - 1 & (x_1 \dots x_{n-1} \equiv y_1 \dots y_{n-1}) \\ - 1 & (x_1 \dots x_{n-1} \not\equiv y_1 \dots y_{n-1}) , \end{cases}$$

so that

$$T_n = pT_{n-1} - \sum_{\substack{x_1, \dots, x_{n-1} \\ y_1, \dots, y_{n-1}}} e(x_1 + \dots + x_{n-1} - y_1 - \dots - y_{n-1}) .$$

Hence

$$(10) \quad T_n = pT_{n-1} - 1 .$$

Now

$$T_1 = \sum_{x=y} e(x - y) = p - 1 , \quad T_2 = p(p - 1) - 1 = p^2 - p - 1$$

and generally

$$(11) \quad T_n = p^n - p^{n-1} - \dots - 1 .$$

Thus (9) becomes

$$(12) \quad \sum_c |S_n(c)|^2 = p^{n+1} - p^n - \dots - p$$

and (8) follows at once.

It follows from (12) that

$$S_n(c) = o(p^{n/2})$$

cannot hold for all c .

3. Returning to (4) we shall now show that

$$(13) \quad S(c) = O(p^{11/8}) .$$

It is convenient to put

$$S(a, b, c) = \sum_{x,y} e(ax + by + cx'y') .$$

Then

$$(14) \quad \sum_{a=1}^{p-1} \sum_{b=0}^{p-1} \sum_{c=0}^{p-1} |S(a, b, c)|^4 = p^3 N,$$

where N denotes the number of solutions of the system

$$\left\{ \begin{array}{l} x_1 + x_2 \equiv x_3 + x_4 \\ y_1 + y_2 \equiv y_3 + y_4 \\ x'_1 y'_1 + x'_2 y'_2 \equiv x'_3 y'_3 + x'_4 y'_4 \\ x_1 x_2 x_3 x_4 y_1 y_2 y_3 y_4 \not\equiv 0. \end{array} \right.$$

Eliminating x_4, y_4 it follows that N is the number of solutions of

$$(15) \quad \begin{aligned} (x_1 y_1 + x_2 y_2) x_3 y_3 (x_1 + x_2 - x_3) (y_1 + y_2 - y_3) \\ \equiv x_1 y_1 x_2 y_2 [(x_1 + x_2 - x_3) (y_1 + y_2 - y_3) + x_3 y_3] \end{aligned}$$

such that

$$(16) \quad x_1 x_2 x_3 y_1 y_2 y_3 (x_1 + x_2 - x_3) (y_1 + y_2 - y_3) \not\equiv 0.$$

Now by a theorem of Lang and Weil [2] we have

$$N = p^5 + O(p^{5-1/2}),$$

so that (14) becomes

$$(17) \quad \sum_{a=0}^{p-1} \sum_{b=0}^{p-1} \sum_{c=0}^{p-1} |S(a, b, c)|^4 = p^8 + O(p^{15/2}).$$

On the other hand

$$\begin{aligned} \sum_{a=0}^{p-1} \sum_{b=0}^{p-1} \sum_{c=0}^{p-1} |S(a, b, c)|^4 &= |S(0, 0, 0)|^4 + 3 \sum_{a=1}^{p-1} \sum_{b=1}^{p-1} |S(a, b, 0)|^4 \\ &+ 3 \sum_{a=1}^{p-1} |S(a, 0, 0)|^4 + \sum_{a=1}^{p-1} \sum_{b=1}^{p-1} \sum_{c=1}^{p-1} |S(a, b, c)|^4 \\ &= (p-1)^8 + (p-1)^2 + 3(p-1)^5 + (p-1)^2 \sum_{c=1}^{p-1} |S(c)|^4, \end{aligned}$$

so that (17) reduces to

$$(18) \quad \sum_{c=1}^{p-1} |S(c)|^4 = O(p^{11/2}).$$

Clearly (18) implies (13).

4. If an exact formula for

$$\sum_{c=0}^{p-1} |S(c)|^4$$

were available we should presumably be able to prove

$$(19) \quad S(c) = O(p^{5/4}) .$$

In this connection it may be of interest to remark that the sum

$$(20) \quad \sum_{c=0}^{p-1} S^3(c)$$

can be evaluated. Indeed if we put

$$S(a, b, c) = \sum_{x, y} e(ax + by + cx' y') ,$$

then

$$(21) \quad \sum_{a=0}^{p-1} \sum_{b=0}^{p-1} \sum_{c=0}^{p-1} (S(a, b, c))^3 = p^3 N ,$$

where N denotes the number of solutions of the system

$$(22) \quad \left\{ \begin{array}{l} x_1 + x_2 + x_3 \equiv 0 \\ y_1 + y_2 + y_3 \equiv 0 \\ x'_1 y'_1 + x'_2 y'_2 + x'_3 y'_3 \equiv 0 \\ x_1 x_2 x_3 y_1 y_2 y_3 \not\equiv 0 . \end{array} \right.$$

Eliminating x_3, y_3 , we find that (22) reduces to

$$(23) \quad x_1(x_1 + x_2)y_1^2 + (x_1^2 + 3x_1x_2 + x_2^2)y_1y_2 + x_2(x_1 + x_2)y_2^2 \equiv 0$$

together with

$$(24) \quad x_1x_2y_1y_2(x_1 + x_2)(y_1 + y_2) \not\equiv 0 .$$

We may replace (23) by

$$(25) \quad [(x_1 + x_2)y_1 + x_2y_2][x_1y_1 + (x_1 + x_2)y_2] = 0 .$$

If $x_1x_2(x_1 + x_2)y_1 \not\equiv 0$, it is clear from (25) that $y_2 \not\equiv 0$ and $y_1 - y_2 \not\equiv 0$. The two factors in (25) may vanish simultaneously. This will happen when

$$(26) \quad x_1^2 + x_1x_2 + x_2^2 \equiv 0 ,$$

that is when -3 is a quadratic residue of p ; moreover if x_1, x_2 satisfy (26) with $x_1x_2 \not\equiv 0$ then $x_1 + x_2 \not\equiv 0$. Thus the number of solutions of (26) is equal to

$$\left\{ 1 + \left(\frac{-3}{p} \right) \right\} \frac{p-1}{2} .$$

If -3 is a nonresidue we find that

$$(27) \quad N = 2(p-1)^2(p-2),$$

while, if -3 is a residue,

$$(28) \quad N = 2(p-1)^2(p-2) - (p-1)^2.$$

For $p = 3$ we have

$$(29) \quad N = 4,$$

for it is evident from (22) that $x_1 \equiv x_2 \equiv x_3$, $y_1 \equiv y_2 \equiv y_3$.

Combining (27) and (28) we have

$$(30) \quad N = 2(p-1)^2(p-2) - \left\{1 + \left(\frac{-3}{p}\right)\right\} \frac{(p-1)^2}{2} \quad (p > 3).$$

On the other hand, since

$$\begin{aligned} S(0, 0, 0) &= (p-1)^2 S(a, 0, 0) = -(p-1) & (a \neq 0), \\ S(a, b, 0) &= 1 & (ab \neq 0), \end{aligned}$$

we have

$$\begin{aligned} \sum_{a=0}^{p-1} \sum_{b=0}^{p-1} \sum_{c=0}^{p-1} (S(a, b, c))^3 &= (p-1)^6 - 3(p-1)^4 + 3(p-1)^2 \\ &+ \sum_{a=1}^{p-1} \sum_{b=1}^{p-1} \sum_{c=1}^{p-1} (S(a, b, c))^3 \\ &= (p-1)^6 - 3(p-1)^4 + 3(p-1)^2 + (p-1)^2 \sum_{c=1}^{p-1} (S(c))^3. \end{aligned}$$

Therefore, using (21) and (30), we get

$$(31) \quad \begin{aligned} \sum_{c=1}^{p-1} (S(c))^3 &= 2p^3(p-2) - (p-1)^4 \\ &+ 3(p-1)^2 - 3 - \frac{1}{2} \left\{1 + \left(\frac{-3}{p}\right)\right\}. \end{aligned}$$

5. We shall now show that

$$(32) \quad S(c) = O(p^{5/4}).$$

With the notation of § 3 we have, as above,

$$(33) \quad \sum_{a=0}^{p-1} \sum_{b=0}^{p-1} \sum_{c=0}^{p-1} |S(a, b, c)|^4 = p^3 N,$$

where N is the number of solutions of the system

$$(34) \quad \begin{cases} (x_1 + x_2)x_3x_4 \equiv x_1x_2(x_3 + x_4) \\ (y_1 + y_2)y_3y_4 \equiv y_1y_2(y_3 + y_4) \\ x_1y_1 + x_2y_2 \equiv x_3y_3 + x_4y_4 \\ x_1x_2x_3x_4y_1y_2y_3y_4 \not\equiv 0 . \end{cases}$$

Note that we have replaced each x_j, y_j by its reciprocal (mod p).

If we put

$$x_3 = x_1u_1, \quad x_4 = x_2u_2, \quad y_3 = y_1v_1, \quad y_4 = y_2v_2,$$

(34) becomes

$$(35) \quad \begin{cases} (x_1 + x_2)u_1u_2 \equiv x_1u_1 + x_2u_2 \\ (y_1 + y_2)v_1v_2 \equiv y_1v_1 + y_2v_2 \\ x_1y_1 + x_2y_2 \equiv x_1y_1u_1v_1 + x_2y_2u_2v_2 \\ x_1x_2y_1y_2u_1u_2v_1v_2 \not\equiv 0 . \end{cases}$$

Now put $x_2 = x_1x, y_2 = y_1y$ and (35) reduces to

$$(36) \quad \begin{cases} (1 + x)u_1u_2 \equiv u_1 + xu_2 \\ (1 + y)v_1v_2 \equiv v_1 + yv_2 \\ 1 + xy \equiv u_1v_1 + xyu_2v_2 \\ xyx_1y_1u_1v_1u_2v_2 \not\equiv 0 . \end{cases}$$

Finally, eliminating x, y we get the single equation

$$(37) \quad \frac{(1 - u_1)(1 - v_1)(1 - u_1v_1)}{u_1v_1} + \frac{(1 - u_2)(1 - v_2)(1 - u_2v_2)}{u_2v_2} \equiv 0$$

subject to

$$(38) \quad x_1y_1u_1v_1u_2v_2 \not\equiv 0 .$$

It should be noted that for fixed u_1, v_1, u_2, v_2 satisfying (37), x, y are uniquely determined by (36) unless $u_1 \equiv u_2 \equiv v_1 \equiv v_2 \equiv 1$; also we find that the forbidden cases $xy \equiv 0$ or xy "infinite" contribute $O(p^2)$.

Let $N'(k)$ denote the number of solutions $u, v \neq 0$ of

$$(39) \quad (1 - u)(1 - v)(1 - uv) \equiv kuv$$

and let $N(k)$ denote the total number of solutions of (39), so that

$$N(k) = N'(k) + O(1) .$$

Then clearly the number of nonzero solutions of (37) is equal to

$$(40) \quad \sum_{k=0}^{p-1} N(k)N(-k) + O(p^2) .$$

Let $\psi(a)$ denote the Legendre symbol (a/p) . Then for fixed u and k , the number of solutions of (39) is equal to

$$1 + \psi\{(1 + ku - u^2)^2 - 4u(1 - u)^2\},$$

so that

$$N(k) = p + \sum_{u=0}^{p-1} \psi(f(k, u)),$$

where

$$(41) \quad f(k, u) = (1 + ku - u^2)^2 - 4u(1 - u)^2.$$

Thus (40) becomes

$$(42) \quad p^3 + 2p \sum_{k=0}^{p-1} \sum_{u=0}^{p-1} \psi(f(k, u)) \\ + \sum_{k=0}^{p-1} \sum_{u=0}^{p-1} \sum_{v=0}^{p-1} \psi(f(k, u))\psi(f(-k, v)) + O(p^2).$$

Since $f(k, u)$ is a quadratic in k we have

$$\sum_{k=0}^{p-1} \psi(f(k, u)) = -1$$

unless $u(1 - u) \equiv 0$. It follows that

$$(43) \quad \sum_{k=0}^{p-1} \sum_{u=0}^{p-1} \psi(f(k, u)) = O(p^2).$$

Consider next the sum

$$\sum_{u=0}^{p-1} \psi(f(k, u)).$$

It is easily seen from (41) that for fixed k , $f(k, u)$ is the square of a polynomial in u only when $k \equiv 0$. We therefore have the estimate

$$(44) \quad \sum_{u=0}^{p-1} \psi(f(k, u)) = O(p^{1/2}),$$

so that

$$(45) \quad \sum_{k=0}^{p-1} \sum_{u=0}^{p-1} \sum_{v=0}^{p-1} \psi(f(k, u))\psi(f(-k, v)) = O(p^2).$$

Substituting from (43) and (45) in (42) we see that the number of nonzero solutions (37) is

$$p^3 + O(p^2).$$

Therefore N , the number of solutions of (34) is

$$p^5 + O(p^4)$$

and (33) becomes

$$\sum_{a=0}^{p-1} \sum_{b=0}^{p-1} \sum_{c=0}^{p-1} |S(a, b, c)|^4 = p^8 + O(p^7);$$

since $S(0, 0, 0) = p^2$,

$$S(a, b, c) = S(1, 1, abc) \quad (abc \not\equiv 0)$$

and there are $(p-1)^2$ terms $S(a, b, c)$ in the sum that give the same $S(1, 1, c)$, (32) now follows immediately.

Note that, except for (44), the proof is elementary.

REFERENCES

1. L. Carlitz and S. Uchiyama, *Bounds for exponential sums*, Duke Math. J. **24** (1957), 37-41.
2. Serge Lang and Ander Weil, *Number of points of varieties in finite fields*, Amer. J. Math. **76** (1953), 819-827.
3. L. J. Mordell, *On a special polynomial congruence and exponential sum*, Calcutta Mathematical Society Golden Jubilee Commemoration Volume (1958/59), Part I, pp. 29-32.
4. A. Weil, *Some exponential sums*, Proc. Nat. Acad. Sci. **34** (1949), 204-207.

PACIFIC JOURNAL OF MATHEMATICS

EDITORS

H. SAMELSON

Stanford University
Stanford, California

R. M. BLUMENTHAL

University of Washington
Seattle, Washington 98105

J. DUGUNDJI

University of Southern California
Los Angeles, California 90007

*RICHARD ARENS

University of California
Los Angeles, California 90024

ASSOCIATE EDITORS

E. F. BECKENBACH

B. H. NEUMANN

F. WOLF

K. YOSIDA

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
CALIFORNIA RESEARCH CORPORATION
SPACE TECHNOLOGY LABORATORIES
NAVAL ORDNANCE TEST STATION

Mathematical papers intended for publication in the *Pacific Journal of Mathematics* should be typewritten (double spaced). The first paragraph or two must be capable of being used separately as a synopsis of the entire paper. It should not contain references to the bibliography. No separate author's resumé is required. Manuscripts may be sent to any one of the four editors. All other communications to the editors should be addressed to the managing editor, Richard Arens, at the University of California, Los Angeles, California 90024.

50 reprints per author of each article are furnished free of charge; additional copies may be obtained at cost in multiples of 50.

The *Pacific Journal of Mathematics* is published quarterly, in March, June, September, and December. Effective with Volume 13 the price per volume (4 numbers) is \$18.00; single issues, \$5.00. Special price for current issues to individual faculty members of supporting institutions and to individual members of the American Mathematical Society: \$8.00 per volume; single issues \$2.50. Back numbers are available.

Subscriptions, orders for back numbers, and changes of address should be sent to Pacific Journal of Mathematics, 103 Highland Boulevard, Berkeley 8, California.

Printed at Kokusai Bunken Insatsusha (International Academic Printing Co., Ltd.), No. 6, 2-chome, Fujimi-cho, Chiyoda-ku, Tokyo, Japan.

PUBLISHED BY PACIFIC JOURNAL OF MATHEMATICS, A NON-PROFIT CORPORATION

The Supporting Institutions listed above contribute to the cost of publication of this Journal, but they are not owners or publishers and have no responsibility for its content or policies.

* Basil Gordon, Acting Managing Editor until February 1, 1966.

David R. Arterburn and Robert James Whitley, <i>Projections in the space of bounded linear operators</i>	739
Robert McCallum Blumenthal, Joram Lindenstrauss and Robert Ralph Phelps, <i>Extreme operators into $C(K)$</i>	747
L. Carlitz, <i>A note on multiple exponential sums</i>	757
Joseph A. Cima, <i>A nonnormal Blaschke-quotient</i>	767
Paul Civin and Bertram Yood, <i>Lie and Jordan structures in Banach algebras</i>	775
Luther Elic Claborn, <i>Dedekind domains: Overrings and semi-prime elements</i>	799
Luther Elic Claborn, <i>Note generalizing a result of Samuel's</i>	805
George Bernard Dantzig, E. Eisenberg and Richard Warren Cottle, <i>Symmetric dual nonlinear programs</i>	809
Philip J. Davis, <i>Simple quadratures in the complex plane</i>	813
Edward Richard Fadell, <i>On a coincidence theorem of F. B. Fuller</i>	825
Delbert Ray Fulkerson and Oliver Gross, <i>Incidence matrices and interval graphs</i>	835
Larry Charles Grove, <i>Tensor products over H^*-algebras</i>	857
Deborah Tepper Haimo, <i>L^2 expansions in terms of generalized heat polynomials and of their Appell transforms</i>	865
I. Martin (Irving) Isaacs and Donald Steven Passman, <i>A characterization of groups in terms of the degrees of their characters</i>	877
Donald Gordon James, <i>Integral invariants for vectors over local fields</i>	905
Fred Krakowski, <i>A remark on the lemma of Gauss</i>	917
Marvin David Marcus and H. Minc, <i>A subdeterminant inequality</i>	921
Kevin Mor McCrimmon, <i>Norms and noncommutative Jordan algebras</i>	925
Donald Earl Myers, <i>Topologies for Laplace transform spaces</i>	957
Olav Njstad, <i>On some classes of nearly open sets</i>	961
Milton Philip Olson, <i>A characterization of conditional probability</i>	971
Barbara Osofsky, <i>A counter-example to a lemma of Skornjakov</i>	985
Sidney Charles Port, <i>Ratio limit theorems for Markov chains</i>	989
George A. Reid, <i>A generalisation of W^*-algebras</i>	1019
Robert Wells Ritchie, <i>Classes of recursive functions based on Ackermann's function</i>	1027
Thomas Lawrence Sherman, <i>Properties of solutions of nth order linear differential equations</i>	1045
Ernst Snapper, <i>Inflation and deflation for all dimensions</i>	1061
Kondagunta Sundaresan, <i>On the strict and uniform convexity of certain Banach spaces</i>	1083
Frank J. Wagner, <i>Maximal convex filters in a locally convex space</i>	1087
Joseph Albert Wolf, <i>Translation-invariant function algebras on compact groups</i>	1093