PACIFIC JOURNAL OF MATHEMATICS
Vol. 15, No. 3, 1965

A NOTE ON MULTIPLE EXPONENTIAL SUMS

L. CARLITZ

Put

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

Where $e(x) = e^{2\pi i/p}$ **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**

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

where $\psi(a)$ **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

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

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

Since

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

it follows that

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

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

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

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.

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

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

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

But

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

so that

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

It follows at once from (5) that

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

so that we have proved (3).

2. Generalizing (4) we define

$$(7)\qquad S_n(c) = \sum_{x_1,\cdots,x_n=1}^{p-1} e(x_1 + \cdots + x_n + cx_1' \cdots x_n') .$$

We shall show that

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

Exactly as above we have

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

where the summation is over all x_j, y_j such that

$$x_1 x_2 \cdots x_n \equiv y_1 y_2 \cdots y_n , \qquad x_j \not\equiv 0 , \quad y_j \not\equiv 0 \pmod p) .$$

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

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

The inner sum is equal to

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

so that

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

Hence

$$T_n = pT_{n-1} - 1 \,. \tag{10}$$

Now

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

and generally

$$T_n = p^n - p^{n-1} - \cdots - 1 \,. \tag{11}$$

Thus (9) becomes

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

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

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

It is convenient to put

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

Then

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

where N denotes the number of solutions of the system

$$\begin{cases} x_1 + x_2 \equiv x_3 + x_4 \\ y_1 + y_2 \equiv y_3 + y_4 \\ x_1'y_1' + x_2'y_2' \equiv x_3'y_3' + x_4'y_4' \\ x_1x_2x_3x_4y_1y_2y_3y_4 \not\equiv 0. \end{cases}$$

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

$$\begin{aligned}(x_1y_1 + x_2y_2)x_3y_3(x_1 + x_2 - x_3)(y_1 + y_2 - y_3) \\ \equiv x_1y_1x_2y_2[(x_1 + x_2 - x_3)(y_1 + y_2 - y_3) + x_3y_3]\end{aligned} \tag{15}$$

such that

$$x_1x_2x_3y_1y_2y_3(x_1 + x_2 - x_3)(y_1 + y_2 - y_3) \not\equiv 0 . \tag{16}$$

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

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

so that (14) becomes

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

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

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

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

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

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

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

can be evaluated. Indeed if we put

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

then

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

where N denotes the number of solutions of the system

$$\begin{cases} x_1 + x_2 + x_3 \equiv 0 \\ y_1 + y_2 + y_3 \equiv 0 \\ x_1'y_1' + x_2'y_2' + x_3'y_3' \equiv 0 \\ x_1x_2x_3y_1y_2y_3 \not\equiv 0 . \end{cases} \tag{22}$$

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

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

together with

$$x_1x_2y_1y_2(x_1 + x_2)(y_1 + y_2) \not\equiv 0 . \tag{24}$$

We may replace (23) by

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

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

$$x_1^2 + x_1x_2 + x_2^2 \equiv 0 , \tag{26}$$

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

$$N = 2(p-1)^2(p-2) , \tag{27}$$

while, if -3 is a residue,

$$N = 2(p-1)^2(p-2) - (p-1)^2 . \tag{28}$$

For $p = 3$ we have

$$N = 4 , \tag{29}$$

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

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

On the other hand, since

$$S(0, 0, 0) = (p-1)^2 S(a, 0, 0) = -(p-1) \qquad (a \not\equiv 0) ,$$
$$S(a, b, 0) = 1 \qquad (ab \not\equiv 0) ,$$

we have

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

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

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

5. We shall now show that

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

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

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

where N is the number of solutions of the system

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

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

If we put

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

(34) becomes

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

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

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

Finally, eliminating x, y we get the single equation

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

subject to

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

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, $v \not\equiv 0$ of

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

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

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

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

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

Thus (40) becomes

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

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

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

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

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

so that

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

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

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

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.