THE HYPER-KLOOSTERMAN SUM

Autor(en): **Weinstein, Lenard**

Objekttyp: **Article**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **27 (1981)**

Heft 1-2: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **21.09.2024**

Persistenter Link: https://doi.org/10.5169/seals-51738

THE HYPER-KLOOSTERMAN SUM

by Lenard WEINSTEIN

1. INTRODUCTION

Deligne, [1], has recently proved the very deep theorem on the bound of the Hyper-Kloosterman sum. His estimate results from his solutions of the strong forms of the Weil conjectures.

The Hyper-Kloosterman sum is defined:

$$S(a_1, \ldots, a_k; p) = \sum e\left(\frac{a_1 x_1 + \ldots + a_k x_k}{p}\right)$$

where $a_1, \ldots, a_k, \alpha$ are non-zero elements of the odd prime field F_p, and the summation runs through the k variables $x_i \in F_p$ with the relation $\prod x_i = \alpha$.

Deligne has shown:

$$|S(a_1, \ldots, a_k; p)| \leqslant k p^{\frac{k-1}{2}}.$$

Here, we prove the following generalization for the bound of the Hyper-Kloosterman sum. Define:

$$S(a_1, \ldots, a_k; q) = \sum e\left(\frac{a_1 x_1 + \ldots + a_k x_k}{q}\right),$$

where $a_1, \ldots, a_k$ are arbitrary integers, q a positive integer, and the summation runs through the k variables x_i, $0 < x_i \leqslant q$, x_i relatively prime to q, with the relation $\prod x_i \equiv 1 \pmod{q}$.

We show:

THEOREM 1. *Let q be an odd positive integer. Then:*

$$|S(a_1, \ldots, a_k; q)| \leqslant k^{v(q)} q^{\frac{k-1}{2}} (a_1, a_k, q)^{1/2} \ldots (a_{k-1}, a_k, q)^{1/2}$$

where $v(q)$ is the number of different prime factors of q.

THEOREM 2. *Let* q *be an even positive integer. Then:*

$$|S(a_1, \ldots, a_k; q)| \leqslant 2^{\frac{k+1}{2}} k^{v(q)} q^{\frac{k-1}{2}} (a_1, a_k, q)^{1/2} \ldots (a_{k-1}, a_k, q)^{1/2}.$$

Estermann, [2], has dealt with the case of the Kloosterman sum.

2. LEMMAS

Lemma 1. Consider the congruence:

$$x^k \equiv a \pmod{p^m}$$

where k, m are positive integers, a is an integer, p a prime and $(a, p) = 1$. Then:

1. If $p > 2$, this congruence has at most k incongruent solutions mod p^m.
2. If $p = 2$ and k is odd, then this congruence has exactly 1 solution mod p^m.
3. If $p = 2$, and $k = 2^r l$, $r > 1$, l odd, then this congruence has at most min $\{2^{r+1}, p^m\}$ solutions mod p^m.

Proof: This is essentially found on pp. 115, 119 of [3].

Lemma 2. Let p be a prime, and m, n positive integers, $\frac{1}{2} m \leqslant n < m$. Let $y_1, \ldots, y_{k-1}, z_1, \ldots, z_{k-1}$ be integers; $p \nmid y_1, \ldots, p \nmid y_{k-1}$. Define $[y_1, \ldots, y_{k-1}; p^m]$ as that integer y, $0 < y < p^m$ such that $y(y_1 \ldots y_{k-1}) \equiv 1 \pmod{p^m}$. Then:

$$\begin{aligned}[y_1 + p^n z_1, \ldots, y_{k-1} + p^n z_{k-1}; p^m] &\equiv [y_1, \ldots, y_{k-1}; p^m] \\ &- [y_1; p^m]^2 [y_2; p^m] \ldots [y_{k-1}; p^m] p^n z_1 \\ &\quad \cdot \\ &\quad \cdot \\ &\quad \cdot \\ &- [y_1; p^m] \ldots [y_{k-2}; p^m] [y_{k-1}; p^m]^2 p^n z_{k-1} \pmod{p^m}\end{aligned}$$

Proof: This follows from the relation

$$[y_1; p^m] \ldots [y_{k-1}; p^m] \equiv [y_1, \ldots, y_{k-1}; p^m] \pmod{p^m}$$

and Lemma 1 of [2].

Lemma 3. Let p be a prime, m, n positive integers, $m = 2n + 1$. Let $y_1, \ldots, y_{k-1}, z_1, \ldots, z_{k-1}$ be integers; $p \nmid y_1, \ldots, p \nmid y_{k-1}$. Then

$$
\begin{aligned}
[y_1 + p^n z_1, \ldots, y_{k-1} + p^n z_{k-1}; p^m] \equiv {} & [y_1, \ldots, y_{k-1}; p^m] \\
& + [y_1; p^m]^3 [y_2; p^m] \cdots [y_{k-1}; p^m]\, p^{2n} z_1^2 \\
& \quad \vdots \\
& + [y_1; p^m] \cdots [y_{k-2}; p^m] [y_{k-1}; p^m]^3 p^{2n} z_{k-1}^2 \\
& - [y_1; p^m]^2 [y_2; p^m] \cdots [y_{k-1}; p^m]\, p^n z_1 \\
& \quad \vdots \\
& - [y_1; p^m] \cdots [y_{k-2}; p^m] [y_{k-1}; p^m]^2 p^n z_{k-1} \\
& + [y_1; p^m]^2 [y_2; p^m]^2 [y_3; p^m] \cdots [y_{k-1}; p^m]\, p^{2n} z_1 z_2 \\
& \quad \vdots \\
& + [y_1; p^m]^2 [y_2; p^m] \cdots [y_{k-2}; p^m] [y_{k-1}; p^m]^2\, p^{2n} z_1 z_{k-1} \\
& + [y_1; p^m] [y_2; p^m]^2 [y_3; p^m]^2 [y_4; p^m] \cdots [y_{k-1}; p^m]\, p^{2n} z_2 z_3 \\
& \quad \vdots \\
& + [y_1; p^m] [y_2; p^m]^2 [y_3; p^m] \cdots [y_{k-2}; p^m] [y_{k-1}; p^m]^2\, p^{2n} z_2 z_{k-1} \\
& \quad \vdots \\
& + [y_1; p^m] \cdots [y_{k-3}; p^m] [y_{k-2}; p^m]^2 [y_{k-1}; p^m]^2\, p^{2n} z_{k-2} z_{k-1} \\
& \pmod{p^m}
\end{aligned}
$$

Proof: This follows from Lemma 5 of [2].

Lemma 4. Let $p > 2$ be a prime, and n a positive integer. Let a, h be integers. Then:

$$\left| \sum_{0 \leq z < p^{n+1}} e(az^2p^{-1} + hzp^{-n-1}) \right| = \begin{cases} 0 & p^n \nmid h \\ p^{n+1/2} & p^n \mid h, \quad p \nmid a \\ p^{n+1} & p^{n+1} \mid h, \quad p \mid a \\ 0 & p^{n+1} \nmid h, \quad p \mid a . \end{cases}$$

Proof: The first two parts of this lemma are Lemma 5 of [2]. The last two parts are trivial.

3. Proof of Theorems 1 and 2

PROPOSITION 1. *Let* p *be a prime,* m *a positive integer and* $a_1, .. a_k.,$ *integers such that*

$$(a_1, a_k, p^m) = \dots = (a_{k-1}, a_k, p^m) = p^h \quad 0 \leqslant h < m .$$

Then

$$S(a_1, \dots, a_k; p^m) = (p^h)^{k-1} S(a_1 p^{-h}, \dots, a_k p^{-h}; p^{m-h})$$

Proof: The proof is similar to that of [2], page 85 bottom.

PROPOSITION 2. *Let* m, n *be positive integers* $\frac{1}{2}m \leqslant n < m,$ p *a prime, and* $a_1, \dots, a_k$ *integers such that* $(a_1, a_k; p^m) = 1.$ *Then:*

$$| S(a_1, \dots, a_k; p^m) | \leqslant A(p^n)^{k-1}$$

where

$$A = \begin{cases} k & \text{if } p > 2 . \\ 1 & \text{if } p = 2 \text{ and } k \text{ is odd} . \\ \min\{2^{r+1}, p^m\} & \text{if } p = 2 \text{ and } k = 2^r l , \\ & \quad r > 1 \text{ and } l \text{ odd} . \end{cases}$$

Proof: Let us assume throughout this proposition that $S(a_1, \dots, a_k; p^m) \neq 0$, or else we are done.

Now we have the identity

$$\sum_{\substack{0 < x_1, \ldots, x_{k-1} \leq p^m \\ p \nmid x_1, \ldots, p \nmid x_{k-1}}} f(x_1, \ldots, x_{k-1})$$

$$= \sum_{\substack{0 < y_1, \ldots, y_{k-1} \leq p^n \\ p \nmid y_1, \ldots, p \nmid y_{k-1}}} \sum_{0 \leq z_1, \ldots, z_{k-1} < p^{m-n}} f(y_1 + p^n z_1, \ldots, y_{k-1} + p^n z_{k-1}).$$

Letting

$$f(x_1, \ldots, x_{k-1}) = e\left(\frac{a_1 x_1 + \ldots + a_{k-1} x_{k-1} + a_k [x_1, \ldots, x_{k-1}; p^m]}{p^m}\right)$$

we see, using Lemma 2

$$S(a_1, \ldots, a_k; p^m)$$

$$= \sum_{\substack{0 < y_1, \ldots, y_{k-1} \leq p^n \\ p \nmid y_1, \ldots, p \nmid y_{k-1}}} e\left(\frac{a_1 y_1 + \ldots + a_{k-1} y_{k-1} + a_k [y_1, \ldots, y_{k-1}; p^m]}{p^m}\right)$$

$$\sum_{0 \leq z_1 < p^{m-n}} e(\{a_1 - a_k [y_1; p^m]^2 \ldots [y_{k-1}; p^m]\} p^{n-m} z_1)$$

$$\vdots$$

$$\sum_{0 \leq z_{k-1} < p^{m-n}} e(\{a_{k-1} - a_k [y_1; p^m] \ldots [y_{k-1}; p^m]^2\} p^{n-m} z_{k-1}).$$

Now since we have assumed $S(a_1, \ldots, a_k; p^m) \neq 0$, the inner sums above must not equal 0. Thus

$$p^{m-n} \mid a_1 - a_k [y_1; p^m]^2 \ldots [y_{k-1}; p^m]$$

$$\vdots$$

$$p^{m-n} \mid a_{k-1} - a_k [y_1; p^m] \ldots [y_{k-1}; p^m]^2 .$$

These congruences imply, since $(a_1, a_k, p^m) = 1$, also $(a_2, a_k, p^m) = \ldots = (a_{k-1}, a_k, p^m) = 1$, and moreover

$$p \nmid a_1, \ldots, p \nmid a_k .$$

Now we have

$$
\begin{aligned}
&| S(a_1, \ldots, a_k; p^m) | \\
\leqslant (p^{m-n})^{k-1} & \sum_{\substack{0 < y_1, \ldots, y_{k-1} \leq p^n \\ p \nmid y_1, \ldots, p \nmid y_{k-1} \\ a_1 \equiv a_k [y_1; p^m]^2 \ldots [y_{k-1}; p^m] \pmod{p^{m-n}} \\ \vdots \\ a_{k-1} \equiv a_k [y_1; p^m] \ldots [y_{k-1}; p^m]^2 \pmod{p^{m-n}}}} 1 \\
= (p^n)^{k-1} & \sum_{\substack{0 < y_1, \ldots, y_{k-1} \leq p^{m-n} \\ p \nmid y_1, \ldots, p \nmid y_{k-1} \\ a_1 \equiv a_k [y_1; p^m]^2 \ldots [y_{k-1}; p^m] \pmod{p^{m-n}} \\ \vdots \\ a_{k-1} \equiv a_k [y_1; p^m] \ldots [y_{k-1}; p^m]^2 \pmod{p^{m-n}}}} 1
\end{aligned}
$$

Now the congruences in the above sum are easily seen to be equivalent to :

$$
\begin{gathered}
a_1 y_1 \equiv a_2 y_2 \equiv \ldots \equiv a_{k-1} y_{k-1} \pmod{p^{m-n}} \\
y_1^k \equiv [a_1; p^m]^{k-1} a_2 \ldots a_k \pmod{p^{m-n}} .
\end{gathered}
$$

Thus by Lemma 1, the proposition is proved.

Proposition 3. *Let* $p > 2$ *be a prime,* $a_1, \ldots, a_k$ *integers such that* $(a_1, a_k, p^m) = 1$, *where* m *is a positive even integer. Then*

$$
| S(a_1, \ldots, a_k; p^m) | \leqslant k (p^m)^{\frac{k-1}{2}}
$$

Proof: This is Proposition 2, with $n = \dfrac{m}{2}$.

PROPOSITION 4. *Let* $p = 2$, m *a positive integer,* $a_1, \ldots, a_k$ *integers such that* $(a_1, a_k, p^m) = 1$. *Then:*

$$| S(a_1, \ldots, a_k; p^m) | \leqslant A_1 (p^m)^{\frac{k-1}{2}}$$

where

$$A_1 = \begin{cases} 1 & , \text{ if } m \text{ even, } k \text{ odd.} \\ \min\{2^{r+1}, p^m\} & , \text{ if } m \text{ even, } k = 2^r l, r > 1, l \text{ odd.} \\ 2^{\frac{k-1}{2}} & , \text{ if } m \text{ odd, } k \text{ odd.} \\ 2^{\frac{k-1}{2}} \min\{2^{r+1}, p^m\} & , \text{ if } m \text{ odd, } k = 2^r l, \ r > 1, \ l \text{ odd.} \end{cases}$$

Proof: This follows from Proposition 2 with $n = m - [\frac{1}{2} m]$.

PROPOSITION 5. *Let* $p > 2$ *be a prime,* $a_1, \ldots, a_k$ *integers. Then*

$$| S(a_1, \ldots, a_k; p) | \leqslant k p^{\frac{k-1}{2}} (a_1, a_k; p)^{1/2} \ldots (a_{k-1}, a_k, p)^{1/2}$$

Proof: If $p \nmid a_1 \ldots a_k$ this is Deligne's theorem. Therefore suppose, without loss of generality that $p \mid a_k, \ldots, p \mid a_{k-i+1}$ where $i \geqslant 1$. Thus:

$$\begin{aligned} S(a_1, \ldots, a_k; p) &= (p-1)^{i-1} \sum_{0 < x_1 < p} e\left(\frac{a_1 x_1}{p}\right) \ldots \sum_{0 < x_{k-i} < p} e\left(\frac{a_{k-i} x_{k-i}}{p}\right) \\ &= (p-1)^{i-1} (-1)^{k-i} \end{aligned}$$

and so the proposition is proved.

PROPOSITION 6. *Let* $p > 2$ *be a prime and* $m > 1$ *an odd positive integer. Then:*

$$| S(a_1, \ldots, a_k; p^m) | \leqslant k (p^m)^{\frac{k-1}{2}} (a_1, a_k, p^m)^{1/2} \ldots (a_{k-1}, a_k, p^m)^{1/2} .$$

Proof: Let us assume throughout this proposition that $S(a_1, \ldots, a_k; p^m) \neq 0$, or else we are done. Let $\dfrac{m-1}{2} = n > 0$.

Now we have the identity:

$$\sum_{\substack{0<x_1,\ldots,x_{k-1}\leq p^{2n+1}\\ p\nmid x_1,\ldots,p\nmid x_{k-1}}} f(x_1,\ldots,x_{k-1})$$

$$= \sum_{\substack{0<y_1,\ldots,y_{k-1}\leq p^n\\ p\nmid y_1,\ldots,p\nmid y_{k-1}}} \quad \sum_{0\leq z_1,\ldots,z_{k-1}<p^{n+1}} f(y_1+p^n z_1,\ldots,y_{k-1}+p^n z_{k-1}).$$

Letting

$$f(x_1,\ldots,x_{k-1}) = e\left(\frac{a_1x_1+\ldots+a_{k-1}x_{k-1}+a_k[x_1,\ldots,x_{k-1};p^m]}{p^m}\right)$$

we see, using Lemma 3

$$S(a_1,\ldots,a_k;p^m)$$

$$= \sum_{\substack{0<y_1,\ldots,y_{k-1}\leq p^n\\ p\nmid y_1,\ldots,p\nmid y_{k-1}}} e\left(\frac{a_1y_1+\ldots+a_{k-1}y_{k-1}+a_k[y_1,\ldots,y_{k-1};p^m]}{p^m}\right)$$

$$\sum_{0\leq z_{k-1}<p^{n+1}} e(\{a_{k-1}-a_k[y_1;p^m]\ldots[y_{k-1};p^m]^2\}p^{-n-1}z_{k-1}$$

$$+[y_1;p^m]\ldots[y_{k-1};p^m]^3a_kp^{-1}z_{k-1}^2)$$

.
.
.

$$\sum_{0\leq z_1<p^{n+1}} e(\{a_1-a_k[y_1;p^m]^2\ldots[y_{k-1};p^m]$$

$$+a_k[y_1;p^m]^2[y_2;p^m]^2\ldots[y_{k-1};p^m]z_2p^n$$

.
.
.

$$+a_k[y_1;p^m]^2[y_2;p^m]\ldots[y_{k-1};p^m]^2z_{k-1}p^n\}\ p^{-n-1}z_1$$

$$+a_k[y_1;p^m]^3\ldots[y_{k-1};p^m]\,z_2^1p^{-1})$$

Since $S(a_1,\ldots,a_k,p^m)$ is assumed to be non-zero, we see by Lemma 4 that:

$$p^n \mid \{ a_1 - a_k [y_1; p^m]^2 \dots [y_{k-1}; p^m] + a_k [y_1; p^m]^2 [y_2; p^m]^2 \dots [y_{k-1}; p^m] z_2 p^n$$

$$\vdots$$

$$+ a_k [y_1; p^m]^2 [y_2; p^m] \dots [y_{k-1}; p^m]^2 z_{k-1} p^n \}$$

$$\vdots$$

$$p^n \mid \{ a_{k-1} - a_k [y_1; p^m] \dots [y_{k-1}; p^m]^2 \} .$$

Now let us assume $(a_1, a_k, p^m) = 1$. By reasoning similar to that of Proposition 2, we see that

$$(a_2, a_k, p^m) = \dots = (a_{k-1}, a_k, p^m) = 1 ,$$

and that $p \nmid a_k$. Thus by Lemma 4:

$$| S(a_1, \dots, a_k; p^m) | \leqslant (p^{n+1/2})^{k-1} \sum_{\substack{0 < y_1, \dots, y_{k-1} \leq p^n \\ p \nmid y_1, \dots, p \nmid y_{k-1}}} 1$$

$$a_1 \equiv a_k [y_1; p^m]^2 \dots [y_{k-1}; p^m] \pmod{p^n}$$

$$\vdots$$

$$a_{k-1} \equiv a_k [y_1; p^m] \dots [y_{k-1}; p^m]^2 \pmod{p^n}$$

Now by reasoning as in Proposition 2 we see $p \nmid a_1, \dots, p \nmid a_{k-1}$, and so by Lemma 1:

$$| S(a_1, \dots, a_k; p^m) | \leqslant k\, p^{(n+1/2)k-1} .$$

Now let us assume

$$(a_1, a_k, p^m) = p^h, \ 0 < h < n+1 ,$$

(if this case is possible.)
Thus $p \mid a_k$, and Lemma 4 now shows:

$$a_1 \equiv a_k [y_1; p^m]^2 \dots [y_{k-1}; p^m] \pmod{p^{n+1}}$$

$$\vdots$$

$$a_{k-1} \equiv a_k [y_1; p^m] \dots [y_{k-1}; p^m] \pmod{p^{n+1}}.$$

Thus:

$$(a_2, a_k, p^m) = \dots = (a_{k-1}, a_k, p^m) = p^h.$$

Thus by Proposition 1, we have:

$$S(a_1, \dots, a_k; p^m) = p^{(k-1)h} S(a_1 p^{-h}, \dots, a_k p^{-h}; p^{m-h}).$$

Now by Proposition 3, 5 and the first part of this proposition, we have:

$$| S(a_1, \dots, a_k; p^m) | \leqslant k\, p^{(k-1)h} (p^{m-h})^{\frac{k-1}{2}} = k (p^m)^{\frac{k-1}{2}} (p^h)^{\frac{k-1}{2}}.$$

Now let us assume

$$(a_1, a_k, p^m) = p^{h_1}, \ h_1 \geqslant n+1.$$

As in the previous argument we see

$$(a_2, a_k, p^m) = p^{h_2}, \quad h_2 \geqslant n+1$$

$$\vdots$$

$$(a_{k-1}, a_k, p^m) = p^{h_{k-1}}, \ h_{k-1} \geqslant n+1.$$

Let $h = \min \{h_1, \dots, h_{k-1}\}$. We may assume $h < m$ or else the result is trivial. Now

$$S(a_1, \dots, a_k; p^m)$$

$$= \sum_{\substack{0 < y_1, \dots, y_{k-1} \leqq p^{m-h} \\ p \nmid y_1, \dots, p \nmid y_{k-1}}} \ \sum_{0 \leqq z_1, \dots, z_{k-1} < p^h} e\left(\frac{a_1 (y_1 + p^{m-h} z_1) + \dots + a_k [y_1 + p^{m-h} z_1, \dots; p^m]}{p^m}\right).$$

Now since $p^m \mid a_1 p^{m-h}, \dots, p^m \mid a_{k-1} p^{m-h}$ and since

$$[y_1 + p^{m-h} z_1, \dots, y_{k-1} + p^{m-h} z_{k-1}; p^m] \equiv [y_1, \dots, y_{k-1}; p^{m-h}] \pmod{p^{m-h}}$$

we have

$$S(a_1, \ldots, a_k; p^m)$$

$$= p^{h(k-1)} \sum_{\substack{0 < y_1, \ldots, y_{k-1} \leq p^{m-h} \\ p \nmid y_1, \ldots, p \nmid y_{k-1}}} e\left(\frac{a_1 p^{-h} y_1 + \ldots + a_k p^{-h} [y_1, \ldots, y_{k-1}; p^{m-h}]}{p^{m-h}}\right)$$

$$= p^{h(k-1)} S(a_1 p^{-h}, \ldots, a_k p^{-h}; p^{m-h}) .$$

Now we may assume without loss of generality that $h = h_1$. Thus by Propositions 3, 5 and the first part of this proposition,

$$| S(a_1, \ldots, a_k; p^m) | \leqslant k\, p^{h(k-1)}\, p^{(m-h)\left(\frac{k-1}{2}\right)}$$

$$= k (p^m)^{\frac{k-1}{2}} (p^h)^{\frac{k-1}{2}} .$$

Proposition 7. *Let* $p > 2$ *be a prime,* m *an even positive integer, and* $a_1, \ldots, a_k$ *integers. Then:*

$$| S(a_1, \ldots, a_k; p^m) | \leqslant k (p^m)^{\frac{k-1}{2}} (a_1, a_k, p^m)^{1/2} \ldots (a_{k-1}, a_k, p^m)^{1/2} .$$

Proof: Using the identity of Proposition 2 and the results of Propositions 3, 5, 6, this is proved as Proposition 6.

Proposition 8. *Let* $p = 2$, m *a positive integer,* $a_1, \ldots, a_k$ *integers. Then*

$$| S(a_1, \ldots, a_k; p^m) | \leqslant 2^{\frac{k+1}{2}} k (p^m)^{\frac{k-1}{2}} (a_1, a_k, p^m)^{1/2} \ldots (a_{k-1}, a_k, p^m)^{1/2} .$$

Proof: This is proved as Proposition 7.

Theorem 1. *Let* q *be a positive odd integer. Then for any integers* $a_1, \ldots, a_k$ *:*

$$| S(a_1, \ldots, a_k; q) | \leqslant k^{v(q)} q^{\frac{k-1}{2}} (a_1, a_k, q)^{1/2} \ldots (a_{k-1}, a_k, q)^{1/2} .$$

Proof: We proceed by induction on q. For $q = 1$ the theorem is trivial. Assume the theorem true for all $S(b_1, \ldots, b_k; q')$, $q' < q$, $b_1, \ldots, b_k$ integers.

Now consider $S(a_1, \ldots, a_k; q)$.

By Propositions 5, 6, 7, we may assume q is not a prime power; hence there exist odd q_1, q_2 such that $q = q_1 q_2$, $(q_1, q_2) = 1$, $q_1 > 1$, $q_2 > 1$. Thus there exist integers a_{k_1}, a_{k_2} such that

$$a_k = a_{k_1} q_2^k + a_{k_2} q_1^k .$$

By the multiplicative property of the Hyper-Kloosterman sum (see Estermann, [2], p. 86) we have

$$S(a_1, \ldots, a_{k-1}, a_k; q) = S(a_1, \ldots, a_{k-1}, a_{k_1}; q_1) \, S(a_1, \ldots, a_{k-1}, a_{k_2}; q_2) .$$

Thus by the inductive assumption

$$\begin{aligned} &| S(a_1, \ldots, a_{k-1}, a_k; q) | \\ &\leqslant k^{v(q_1)} (q_1)^{\frac{k-1}{2}} (a_1, a_{k_1}, q_1)^{1/2} \ldots (a_{k-1}, a_{k_1}, q_1)^{1/2} \\ &\cdot k^{v(q_2)} (q_2)^{\frac{k-1}{2}} (a_1, a_{k_2}, q_2)^{1/2} \ldots (a_{k-1}, a_{k_2}, q_2)^{1/2}. \end{aligned}$$

Since it is easily seen

$$\begin{aligned} (a_1, a_{k_1}, q_1)(a_1, a_{k_2}, q_2) &= (a_1, a_k, q) \\ &\vdots \\ (a_{k-1}, a_{k_1}, q_1)(a_{k-1}, a_{k_2}, q_2) &= (a_{k-1}, a_k, q) \end{aligned}$$

the theorem is proved.

Theorem 2 is proved similarly.

Note. By symmetry, the $(a_1, a_k, q)^{1/2} \ldots (a_{k-1}, a_k, q)^{1/2}$ term in Theorems 1 and 2 may be replaced by

$$\begin{aligned} \min \{ &(a_1, a_k, q)^{1/2} (a_2, a_k, q)^{1/2} \ldots (a_{k-1}, a_k, q)^{1/2} , \\ &(a_1, a_{k-1}, q)^{1/2} (a_2, a_{k-1}, q)^{1/2} \ldots (a_k, a_{k-1}, q)^{1/2} , \\ &\vdots \\ &(a_2, a_1, q)^{1/2} (a_3, a_1, q)^{1/2} \ldots (a_k, a_1, q)^{1/2} \} . \end{aligned}$$

REFERENCES

[1] DELIGNE, P. Séminaire Géométrie Algébrique $4^{1/2}$. *Lecture Notes 569* (1977), pp. 221, 228.
[2] ESTERMANN, T. On Kloosterman's sum. *Mathematika 8* (1961), pp. 83-86.
[3] NAGELL, T. *Number Theory*. New York, John Wiley & Sons, 1951.

(Reçu le 14 juin 1980)

Lenard Weinstein

Department of Mathematics
Temple University
Philadelphia, Pennsylvania 19122