$l_1 = 0, \ldots, l_{h-1} = 0$, $l_h = n_h$ besitzen. Ein Beispiel liefert hierfür der von Besicovitch behandelte Fall $m_k = a_k p_k$ $(k = 1, \ldots, h)$, wobei

$$h \leqslant g, \quad s_{vw} = 0 \quad (v, w = 1, \ldots, h;\ v \neq w), \quad s_{vv} = 1 \quad (v = 1, \ldots, h)$$

wird und (9) mit den k Kongruenzen

$$l_v \equiv 0 \pmod{n_v} \quad (v = 1, \ldots, k)$$

gleichbedeutend ist.

Wenn allgemeiner $\mathfrak{R}$ ein beliebiger reeller algebraischer Zahlkörper endlichen Grades ist, so läßt sich die Bedingung (9) ohne weiteres übertragen, indem man die Hauptideale (m_k) in Primideale zerlegt. Für die Bestimmung von j_k treten jedoch weitere Bedingungen hinzu, die von der Gruppe der Idealklassen und der Einheitengruppe herrühren. Deshalb ergibt sich auf diesem Wege doch kein einfaches Verfahren zur Berechnung von N, wenn nicht gerade $\mathfrak{R}$ der rationale Zahlkörper ist.

Zum Abschluss sei noch darauf hingewiesen, daß die Voraussetzung der Realität der Wurzeln beim Beweise nur an einer Stelle benutzt wurde und dort durch die schwächere Annahme ersetzt werden könnte, daß der Körper $\mathfrak{R}_h$ keine von 1 und -1 verschiedene Einheitswurzel enthält. Diese Annahme ist zugleich notwendig, wie bereits das einfachste Beispiel

$$h = 1, \quad m_1 = -4, \quad n_1 = 4, \quad \varrho_1 = \sqrt[4]{-4} = \pm 1 \pm i, \quad N = 4 \neq 2$$

zeigt.

Literaturverzeichnis

[1] A. S. Besicovitch, *On the linear independence of fractional powers of integers*, J. London Math. Soc. 15 (1940), S. 3–6.

[2] G. Hajós, *Über einfache und mehrfache Bedeckung des n-dimensionalen Raumes mit einem Würfelgitter*, Math. Zeitschr. 47 (1941), S. 427–467.

Eingegangen 12. 1. 1971 (132)

ACTA ARITHMETICA
XXI (1972)

On some exponential sums related to Kloosterman sums

by

L. J. MORDELL

In memory of Professor Waclaw Sierpiński

Write

$$S_1(a, b) = S_1 = \sum_{x=1}^{p-1} e(ax + b\bar{x}), \qquad T_1 = \sum_{x=1}^{p-1} e(ax + b\bar{x}) \left(\frac{x}{p}\right), \tag{1}$$
$$ab \not\equiv 0 \pmod{p},$$

where p is an odd prime number, $e(x) = e(2\pi i x/p)$, and we define $\bar{x}$ by $x\bar{x} \equiv 1 \pmod{p}$ and often write $\bar{x} \equiv 1/x \pmod{p}$, and $\left(\frac{x}{p}\right)$ is the Legendre symbol. It is well known that the Kloosterman sum S_1 satisfies the inequality

$$|S_1| < 2\sqrt{p}, \tag{2}$$

and that no elementary proof is known[1]. However, T_1 can be evaluated by elementary methods and

$$T_1 = 0 \quad \text{if} \quad \left(\frac{ab}{p}\right) = -1,$$
$$T_1 = 2\varepsilon^{-1} \left(\frac{-a}{p}\right) \sqrt{p} \cos(2\pi h/p) \quad \text{if} \quad \left(\frac{ab}{p}\right) = 1, \tag{3}$$

where $\varepsilon = i^{\left(\frac{p-1}{2}\right)^2}$ and h is one solution of

$$h^2 - 4ab \equiv 0 \pmod{p}. \tag{4}$$

This result was first found by Salié [1] in 1931, and another proof has just been given by K. S. Williams [2]. Though their proofs are simple,

[1] Note added in proof by A. Schinzel: An elementary proof has been in the meantime given by S. A. Stiepanov, Trudy Mat. Inst. Stieklov. 112, pp. 346–371.

the essential ideas used can be expressed in an even simpler way which also leads to other results. Salié's result is included in the

THEOREM 1. *Write* $T = \sum e(x)$ *taken over the solutions of* $x^2 \equiv 4ab \pmod p$. *Then if* $\left(\frac{ab}{p}\right) = -1$, $T_1 = T = 0$; *and if* $\left(\frac{ab}{p}\right) = 1$, *then*

$$T_1 = \varepsilon^{-1}\sqrt{p}\left(\frac{-a}{p}\right)T = 2\varepsilon^{-1}\left(\frac{-a}{p}\right)\sqrt{p}\cos(2\pi h/p)$$

where h *is one root of the congruence* $h^2 \equiv 4ab \pmod p$.

Obviously,

$$pT = \sum_{t,x=0}^{p-1} e\{x + t(x^2 - 4ab)\},$$

since the sum in t is zero unless $x^2 - 4ab \equiv 0 \pmod p$. The sum in x is a Gaussian sum and so

$$\sum_x e(x + tx^2) = \varepsilon\sqrt{p}\left(\frac{t}{p}\right)e(-1/4t) \text{ or } 0 \text{ according as } t \not\equiv 0 \text{ or } t \equiv 0.$$

Hence[2]

$$pT = \varepsilon\sqrt{p}\sum e(-1/4t - 4abt)\left(\frac{t}{p}\right) = \varepsilon\sqrt{p}\left(\frac{-b}{p}\right)\sum e(at + b/t)\left(\frac{t}{p}\right)$$

on putting $t \to -t/4b$, and so

$$T_1 = \varepsilon^{-1}\left(\frac{-b}{p}\right)\sqrt{p}\,T.$$

This result is easily generalized. We have

THEOREM 2. *Put* $S = \sum e(x_1)$, *where the summation is extended over all the solutions of*

$$x_1^2 + \ldots + x_n^2 \equiv 4a \pmod p.$$

Suppose first that n *is odd. Then if* $\left(\frac{a}{p}\right) = -1$, $S = 0$, *and if* $\left(\frac{a}{p}\right) = 1$,

$$S = 2\varepsilon^{n-1}p^{\frac{n-1}{2}}\left(\frac{-1}{p}\right)\cos(2\pi h/p)$$

where h *is one solution of* $h^2 \equiv 4a \pmod p$. *If* n *is even,*

$$S = \varepsilon^n p^{\frac{n}{2}-1}S_1(a, 1).$$

(2) Here and hereafter we shall omit the limits of summation which will be 0 to $p-1$ for all variables but 0 may be excluded in obvious cases.

We have

$$pS = \sum_{x,t} e\{x_1 + t(x_1^2 + \ldots + x_n^2 - 4a)\}.$$

The sum is zero if $t \equiv 0$. If $t \not\equiv 0$, on summing for the x, we have

$$pS = \varepsilon^{n/2}p^{n/2}\sum_t e(-4at - 1/4t)\left(\frac{t}{p}\right)^n.$$

The theorem now follows.

Consider next the sums,

$$S_2 = \sum_{x,y} e(ax + by + c\bar{x}\bar{y}), \quad T_2 = \sum_{x,y} e(ax + by + c\bar{x}\bar{y})\left(\frac{x}{p}\right), \tag{5}$$

$$abc \not\equiv 0 \pmod p.$$

It has been conjectured but not proved that $S_2 = O(p)$, but only the estimate $S_2 = O(p^{5/4})$ is known, and this has been found independently by Hooley, Davenport and Carlitz. I have not seen an estimate for T_2, but this is easily found from (3), and we have

THEOREM 3.

$$T_2 = \varepsilon\sqrt{p}\sum_x e(x + 4abc/x^2) = O(p). \tag{6}$$

For on summing for x and applying equation (3) to (5),

$$T_2 = \varepsilon^{-1}\sqrt{p}\left(\frac{-a}{p}\right)\sum_{y,h} e(by + h),$$

where $h^2 \equiv 4ac\bar{y} \pmod p$,

$$= \varepsilon^{-1}\sqrt{p}\left(\frac{-a}{p}\right)\sum_h e(h + 4abc/h^2),$$

and this is the result since this exponential sum is $O(p)$.

The sums (5) suggest the consideration of the more general sum

$$\sum_x e(a_1x_1 + \ldots + a_nx_n + a_{n+1}/x_1 \ldots x_n)\left(\frac{x_1x_2 \ldots x_r}{p}\right), \quad r \leqslant n.$$

There is no loss of generality in taking $a_2 = \ldots = a_{n+1} = 1$ as is obvious on writing $x_2 \to x_2/a_2$, etc., and so we write

$$S_n = \sum_x e(ax_1 + x_2 + \ldots + x_{n+1} + 1/x_1 \ldots x_n)\left(\frac{x_1x_2 \ldots x_r}{p}\right), \tag{7}$$

$$r \leqslant n, \quad a \not\equiv 0 \pmod p.$$

We have now with $\eta = \left(\frac{-a}{p}\right)$, $\zeta = \left(\frac{-1}{p}\right)$,

THEOREM 4. *If* $n = 2m$, $r = m$,

$$S_n/(\varepsilon^{-1}\sqrt{p})^m = \zeta^{m-1}\eta \sum_y e(y_1+\ldots+y_m+4^m a/y_1^2\ldots y_m^2).$$

If $n = 2m+1$, $r = m+1$,

$$S_n/(\varepsilon^{-1}\sqrt{p})^{m+1} = 0 \quad \text{if} \quad \left(\frac{a}{p}\right) = -1,$$

but if $\left(\frac{a}{p}\right) = 1$, *and* $h^2 \equiv 4a \pmod p$,

$$S_n/(\varepsilon^{-1}\sqrt{p})^{m+1} = \zeta^m \eta \sum_{y,h} e(y_1+\ldots+y_m+2^m h/y_1\ldots y_m).$$

Sum (7) for x_1. Then from (3),

$$S_n/\varepsilon^{-1}\sqrt{p} = \eta \sum e(y_1+x_2+\ldots+x_n)\left(\frac{x_2\ldots x_r}{p}\right), \qquad y_1^2 \equiv 4a/x_2\ldots x_n.$$

Substitute for x_n. Then

$$S_n/\varepsilon^{-1}\sqrt{p} = \eta \sum e(y_1+x_2+\ldots+x_{n-1}+4a/y_1^2 x_2\ldots x_{n-1})\left(\frac{x_2\ldots x_r}{p}\right).$$

Sum for x_2. Then

$$S_n/(\varepsilon^{-1}\sqrt{p})^2 = \zeta\eta \sum e(y_1+y_2+x_3+\ldots+x_{n-1})\left(\frac{x_3\ldots x_r}{p}\right),$$

$$y_2^2 \equiv 4^2 a/y_1^2 x_3\ldots x_{n-1}.$$

Substitute for x_{n-1}. Then

$$S_n/(\varepsilon^{-1}\sqrt{p})^2 = \zeta\eta \sum e(y_1+y_2+x_3+\ldots+x_{n-2}+4^2 a/y_1^2 y_2^2 x_3\ldots x_{n-2})\left(\frac{x_3\ldots x_r}{p}\right).$$

We continue the process, summing for x_3, etc.

If $n = 2m$, $r = m$, we come to a stage,

$$S_n/(\varepsilon^{-1}\sqrt{p})^m = \zeta^{m-1}\eta \sum e(y_1+\ldots+y_m+x_{m+1}), \qquad y_m^2 = 4^m a/y_1^2\ldots y_{m-1}^2 x_{m+1}$$
$$= \zeta^{m-1}\eta \sum e(y_1+\ldots+y_m+4^m a/y_1^2\ldots y_m^2).$$

If $n = 2m+1$, $r = m+1$, we come to a stage,

$$S_n/(\varepsilon\sqrt{p})^m = \zeta^{m-1}\eta \sum e(y_1+\ldots+y_m+x_{m+1}+4^m a/y_1^2\ldots y_m^2 x_{m+1})\left(\frac{x_{m+1}}{p}\right).$$

Then summing for x_{m+1},

$$S_n/(\varepsilon^{-1}\sqrt{p})^{m+1} = \zeta^m \eta \sum e(y_1+\ldots+y_m+y_{m+1}),$$

where

$$y_{m+1}^2 \equiv 4^{m+1} a/y_1^2\ldots y_m^2,$$

and so the sum is zero unless $\left(\frac{a}{p}\right) = 1$. If $h^2 \equiv 4a$,

$$y_1\ldots y_{m+1} \equiv \pm 2^m h,$$

and so

$$S_n/(\varepsilon^{-1}\sqrt{p})^{m+1} = \zeta^m \eta \sum_{y,h} e(y_1+\ldots+y_m+2^m h/y_1\ldots y_m), \qquad h^2 \equiv 4a \pmod p.$$

In particular, when $n = 4$,

$$\sum_x e(ax_1+x_2+x_3+x_4+1/x_1x_2x_3x_4)\left(\frac{x_1x_2}{p}\right) = \left(\frac{a}{p}\right)p \sum_y e(y_1+y_2+16a/y_1^2y_2^2);$$

when $n = 5$,

$$\sum_x e(ax_1+x_2+x_3+x_4+x_5+1/x_1x_2x_3x_4x_5)\left(\frac{x_1x_2x_3}{p}\right) = \varepsilon\eta p^{3/2} \sum_{y,h} e(y_1+y_2+4h/y_1y_2).$$

References

[1] Hans Salié, *Über die Kloostermanschen Summen* $S(u, v; q)$, Math. Zeitschr. 34 (1931), pp. 91–109.

[2] K. S. Williams, *Finite transformation formulae involving the Legendre symbol*, Pacific Journ. Math. 34 (1970), pp. 559–568.

UNIVERSITY OF CALGARY, Canada
St. JOHN'S COLLEGE, Cambridge, England

Received on 15. 1. 1971 (144)