# A NOTE ON KLOOSTERMAN SUMS

ALBERT LEON WHITEMAN

**1. Introduction.** In recent years the Kloosterman sum

$$A_k(n) = \sum_{h \bmod k}{}' \exp (2\pi i n(h + \bar{h})/k)$$

has played an increasingly important role in the analytic theory of numbers. The dash $'$ beside the summation symbol indicates that the letter of summation runs only through a reduced residue system with respect to the modulus. The number $\bar{h}$ is defined as any solution of the congruence $h\bar{h} \equiv 1 \pmod{k}$, and $n$ denotes an arbitrary integer. It was shown by Salié[1] almost fifteen years ago that $A_k(n)$ may be evaluated explicitly when $k$ is a power of a prime. Salié's result is given by the following theorem.

THEOREM. *Let $k = p^\alpha$, $\alpha \geqq 2$, $(n, k) = 1$, where $p$ denotes an odd prime. Then,*

(i) *if $\alpha$ is even,*

$$A_k(n) = 2k^{1/2} \cos (4\pi n/k);$$

(ii) *if $\alpha$ is odd,*

$$A_k(n) = \begin{cases} 2(n \mid k)k^{1/2} \cos (4\pi n/k) & \text{for } p \equiv 1 \pmod{4}, \\ -2(n \mid k)k^{1/2} \sin (4\pi n/k) & \text{for } p \equiv 3 \pmod{4}. \end{cases}$$

The symbol $(n \mid k)$ denotes, as is usual, the Legendre symbol.

Salié's proof of his theorem is based upon induction. In the present note a direct proof is given. The method consists in introducing a transformation which expresses the Kloosterman sum in terms of Gauss sums and certain types of Ramanujan sums.

**2. Two lemmas.** A Gauss sum may be defined by

$$G_{h,k} = \sum_{m=0}^{k-1} \exp (2\pi i h m^2/k).$$

We shall find it convenient to write $G$ instead of $G_{1,k}$. The following lemma[2] is classical.

---

Received by the editors October 26, 1944.

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

[2] See, for example, Edmund Landau, *Vorlesungen über Zahlentheorie*, vol. 1, p. 153.

LEMMA 1. *If $k$ is an odd integer and $(h, k)=1$, then*

$$G_{h,k} = (h \mid k)G \tag{1}$$

*and*

$$G = i^{((k-1)/2)^2}k^{1/2}. \tag{2}$$

We shall also need the following lemma.

LEMMA 2. *Let $p$ denote an odd prime; let $n$ and $\alpha$ denote positive integers. Then*

$$\sum_{h \bmod p^\alpha}{}' \exp(2\pi inh/p^\alpha) = \begin{cases} p^\alpha - p^{\alpha-1} \text{ if } p^\alpha \mid n, \\ -p^{\alpha-1} \text{ if } p^\alpha \nmid n \text{ but } p^{\alpha-1} \mid n, \\ 0 \textit{ if } p^{\alpha-1} \nmid n (\alpha > 1). \end{cases} \tag{3}$$

*Furthermore, if $\alpha$ is odd, and if we put $n_1 = n/p^{\alpha-1}$ when $p^{\alpha-1} \mid n$, we have*

$$\sum_{h \bmod p^\alpha}{}' (h \mid p^\alpha) \exp(2\pi inh/p^\alpha) = \begin{cases} 0 \textit{ if } p^\alpha \mid n, \\ i^{((p-1)/2)^2}(n_1 \mid p)p^{\alpha-1/2} \\ \textit{if } p^{\alpha-1} \mid n \textit{ but } p^\alpha \nmid n, \\ 0 \textit{ if } p^{\alpha-1} \nmid n(\alpha > 1). \end{cases} \tag{4}$$

The first part of this lemma follows at once from a well known transformation formula[3] for Ramanujan sums or may easily be proved directly. The second part of the lemma may be established in the following way:

If $p^\alpha \mid n$, then

$$\sum_{h \bmod p^\alpha}{}' (h \mid p^\alpha) \exp(2\pi inh/p^\alpha) = \sum_{h \bmod p^\alpha}{}' (h \mid p^\alpha) = 0.$$

If $p^\alpha \nmid n$ but $p^{\alpha-1} \mid n$, then by (1)

$$\begin{aligned} \sum_{h \bmod p^\alpha}{}' (h \mid p^\alpha) \exp(2\pi inh/p^\alpha) &= \sum_{h \bmod p^\alpha}{}' (h \mid p) \exp(2\pi in_1h/p) \\ &= (n_1 \mid p)p^{\alpha-1}\sum_{h=1}^{p-1} (h \mid p) \exp(2\pi ih/p). \end{aligned}$$

But it is easy to show that[4]

$$G_{1,p} = \sum_{h=1}^{p-1} (h \mid p) \exp(2\pi ih/p). \tag{5}$$

Hence, by (2), the lemma is established in this case. Finally, if $p^{\alpha-1} \nmid n$,

[3] See, for example, Landau, loc. cit., vol. 1, bottom of p. 280.

[4] See, for example, Landau, loc. cit., vol. 1, p. 155.

$$\begin{aligned}\sum_{h \bmod p^\alpha}{}' (h \mid p^\alpha) \exp(2\pi i n h/p^\alpha) \\ &= \sum_{h \bmod p^\alpha}{}' (h + p \mid p^\alpha) \exp(2\pi i n(h+p)/p^\alpha) \\ &= \exp(2\pi i n/p^{\alpha-1}) \sum_{h \bmod p^\alpha}{}' (h \mid p^\alpha) \exp(2\pi i n h/p^\alpha) = 0,\end{aligned}$$

where we have noted that $\exp(2\pi i n/p^{\alpha-1}) \neq 1$ since $p^{\alpha-1} \nmid n$. This completes the proof of Lemma 2.

3. **Proof of Salié's theorem.** Let us first observe that (2) may be written in the form $1 = (-1 \mid k)G^2/k$. Using (1) we may now transform the Kloosterman sum $A_k(n)$ in the following manner.

$$\begin{aligned}A_k(n) &= (-1 \mid k)G^2/k \sum_{h \bmod k}{}' \exp(2\pi i(-n^2 h - \bar{h})/k) \\ &= (-1 \mid k)G/k \sum_{h \bmod k}{}' \exp(2\pi i(-n^2 h - \bar{h})/k) \\ &\qquad \cdot \sum_{m=0}^{k-1} (h \mid k) \exp(2\pi i h m^2/k) \\ &= (-1 \mid k)G/k \sum_{h \bmod k}{}' \sum_{m=0}^{k-1} (h \mid k) \exp(2\pi i h(m^2 - n^2 - \bar{h}^2)/k) \\ &= (-1 \mid k)G/k \sum_{h \bmod k}{}' \sum_{m=0}^{k-1} (h \mid k) \exp(2\pi i h(m^2 - n^2 + 2m\bar{h})/k)\end{aligned}$$

since $m+\bar{h}$ runs through a complete residue system with respect to the modulus $k$ whenever $m$ does. Interchanging signs of summation we get

$$A_k(n) = (-1 \mid k)G/k \sum_{m=0}^{k-1} \exp(4\pi i m/k) \cdot \sum_{h \bmod k}{}' (h \mid k) \exp(2\pi i(m^2 - n^2)h/k). \tag{6}$$

At this point we divide the discussion into two cases according as $\alpha$ is even or odd. For $\alpha$ even, we have

$$A_k(n) = G/p^\alpha \sum_{m=0}^{p^\alpha - 1} \exp(4\pi i m/p^\alpha) \sum_{h \bmod p^\alpha}{}' \exp(2\pi i(m^2 - n^2)h/p^\alpha).$$

Referring to (3) we see that the last sum equals zero except when $p^{\alpha-1} \mid m^2 - n^2$. Now the solutions[5] of the congruence $m^2 \equiv n^2 \pmod{p^\alpha}$

[5] See, for example, G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, pp. 95–96.

are all given by $m \equiv \pm n \pmod{p^\alpha}$, and the solutions of the congruence $m^2 \equiv n^2 \pmod{p^{\alpha-1}}$, $m \bmod p^\alpha$, where $m^2 \not\equiv n^2 \pmod{p^\alpha}$, are $m \equiv \pm n + qp^{\alpha-1} \pmod{p^\alpha}$, $1 \leqq q \leqq p-1$. Hence, applying the first part of Lemma 2, we obtain

$$A_k(n) = G/p^\alpha \Big\{ (p^\alpha - p^{\alpha-1}) \exp(4\pi in/p^\alpha)$$
$$+ (p^\alpha - p^{\alpha-1}) \exp(-4\pi in/p^\alpha) - p^{\alpha-1} \sum_{q=1}^{p-1} \exp(4\pi i(\pm n + qp^{\alpha-1})/p^\alpha) \Big\}$$
$$= 2G \cos(4\pi n/k),$$

which completes the proof of the theorem in the case in which $\alpha$ is even.

We next consider the case which arises when $\alpha$ is odd. For this purpose we return to (6) and obtain

$$A_k(n) = (-1 \mid p^\alpha) G_{1,p^\alpha}/p^\alpha \sum_{m=0}^{p^\alpha - 1} \exp(4\pi im/p^\alpha) \sum_{h \bmod p^\alpha}{}' (h \mid p^\alpha)$$
$$\exp(2\pi i(m^2 - n^2)h/p^\alpha).$$

From (4) we see that the last sum is zero except when $p^{\alpha-1} \mid m^2 - n^2$ but $p^\alpha \nmid m^2 - n^2$. Furthermore, let us observe that the number $n_1$, defined in Lemma 2, is here of the form $\pm 2nq + q^2 p^{\alpha-1}$. Hence, proceeding as we did in the case in which $\alpha$ is even, we get

$$A_k(n) = (-1 \mid p^\alpha) G/p^\alpha \sum_{q=1}^{p-1} \exp(4\pi i(\pm n + qp^{\alpha-1})/p^\alpha)$$
$$\cdot \left\{ i^{((p-1)/2)^2} (\pm 2nq \mid p) p^{\alpha - 1/2} \right\}$$
$$= (-1 \mid p^\alpha) G_{1,p^\alpha}/p^\alpha \Big\{ (n \mid p^\alpha) G_{1,p} p^{\alpha-1}$$
$$\cdot \exp(4\pi in/p^\alpha) \sum_{q=1}^{p-1} (2q \mid p) \exp(4\pi iq/p)$$
$$+ (-n \mid p^\alpha) G_{1,p} p^{\alpha-1} \exp(-4\pi in/p^\alpha) \sum_{q=1}^{p-1} (2q \mid p) \exp(4\pi iq/p) \Big\}$$
$$= (n \mid p^\alpha) G_{1,p^\alpha}/p^\alpha \left\{ (-1 \mid p^\alpha) G_{1,p}^2 p^{\alpha-1} \exp(4\pi in/p^\alpha) \right.$$
$$\left. + G_{1,p}^2 p^{\alpha-1} \exp(-4\pi in/p^\alpha) \right\}.$$

This completes the proof of the theorem in this case in view of Lemma 1.

4. **Concluding remarks.** The reader may have wondered why the case $\alpha = 1$ is excluded in Salié's theorem. The reason is that Salié's

method breaks down in this case as, indeed, does ours. For the sake of completeness we shall now show that when $\alpha=1$ our method leads merely to a transformation formula.

For $k=p$, the last sum in (6) becomes a Gauss sum in view of (5). Thus we have by (1) and (2)

$$\begin{aligned} A_p(n) &= (-1\,|\,p)G/p\sum_{m=0}^{p-1}\exp(4\pi im/p)\sum_{h=1}^{p-1}(h\,|\,p)\exp(2\pi i(m^2-n^2)h/p) \\ &= (-1\,|\,p)G^2/p\sum_{m=0}^{p-1}(m^2-n^2\,|\,p)\exp(4\pi im/p) \\ &= \sum_{m=0}^{p-1}(m^2-4n^2\,|\,p)\exp(2\pi im/p). \end{aligned}$$

Hence, we obtain the transformation formula

$$\sum_{h=1}^{p-1}\exp(2\pi in(h+\bar{h})/p) = \sum_{m=0}^{p-1}(m^2-4n^2\,|\,p)\exp(2\pi im/p),$$

which may, of course, be established directly without much difficulty.

Various sums related to the Kloosterman sum $A_k(n)$ have been evaluated by Salié[6] and Lehmer.[7] The author has verified that the method of this paper may be employed to obtain new derivations of these results.

WASHINGTON, D. C.

---

[6] Loc. cit.

[7] D. H. Lehmer, *On the series for the partition function*, Trans. Amer. Math. Soc. vol. 43 (1938) pp. 271–295.