Canad. Math. Bull. Vol. 16 (3), 1973

THE KLOOSTERMAN SUM REVISITED

BY
KENNETH S. WILLIAMS

1. **Introduction.** Let p be an odd prime, n an integer not divisible by p and α a positive integer. For any integer h with $(h, p^\alpha)=1$, $\bar{h}$ is defined as any solution of the congruence $h\bar{h}\equiv 1 \pmod{p^\alpha}$. The Kloosterman sum $A_{p^\alpha}(n)$ (see for example [4]) is defined by

$$(1.1) \qquad A_{p^\alpha}(n) = \sum_{h \bmod p^\alpha}{}' \exp(2\pi i n(h+\bar{h})/p^\alpha),$$

where the dash (′) indicates that the letter of summation runs only through a reduced residue system with respect to the modulus. When $\alpha=1$ the value of $A_{p^\alpha}(n)$ is unknown in general but Weil [3] has shown that $|A_p(n)|<2p^{1/2}$. When $\alpha\geq 2$ Salié [2] has shown that $A_{p^\alpha}(n)$ can be evaluated explicitly. Salié proved

THEOREM. *Let p be an odd prime, n an integer not divisible by p and α an integer ≥ 2. Then*

$$A_{p^\alpha}(n) = \begin{cases} 2p^{\alpha/2}\cos(4\pi n/p^\alpha), & \text{if } \alpha \text{ is even},\\ 2(n \mid p)p^{\alpha/2}\cos(4\pi n/p^\alpha), & \text{if } \alpha \text{ is odd and } p\equiv 1 \pmod 4,\\ -2(n \mid p)p^{\alpha/2}\sin(4\pi n/p^\alpha), & \text{if } \alpha \text{ is odd and } p\equiv 3 \pmod 4.\end{cases}$$

The symbol $(n \mid p)$ denotes the Legendre symbol.

Salié's proof of his theorem is based upon induction. In a recent paper [5] the author has given a modification of this proof which gives a very short direct evaluation of $A_{p^\alpha}(n)$. Another direct proof has been given by Whiteman [4].

Although the value of $A_p(n)$ is unknown in general the following transformation formula for $A_p(n)$, namely,

$$A_p(n) = \sum_{r \bmod p} (r^2-4 \mid p)\exp(2\pi i n r/p)$$

is well-known (see for example [3], [4]). It is easily proved by collecting together the terms in (1.1) for which $h+\bar{h}$ has the same value r. We have

$$\begin{aligned} A_p(n) &= \sum_{r \bmod p} \sum_{\substack{h \bmod p\\ h+\bar{h}\equiv r \pmod p}}{}' \exp(2\pi i n(h+\bar{h})/p)\\ &= \sum_{r \bmod p} \exp(2\pi i n r/p) \sum_{\substack{h \bmod p\\ h+\bar{h}\equiv r \pmod p}}{}' 1\\ &= \sum_{r \bmod p} \exp(2\pi i n r/p) \sum_{\substack{h \bmod p\\ h^2-rh+1\equiv 0 \pmod p}} 1\\ &= \sum_{r \bmod p} \exp(2\pi i n r/p)\{1+(r^2-4 \mid p)\}\\ &= \sum_{r \bmod p} (r^2-4 \mid p)\exp(2\pi i n r/p), \end{aligned}$$

Received by the editors July 26, 1971.

https://doi.org/10.4153/CMB-1973-057-0 Published online by Cambridge University Press

as

$$\sum_{r \bmod p} \exp(2\pi i n r/p) = 0 \quad \text{for} \quad n \not\equiv 0 \pmod p.$$

In this note we apply this technique to $A_{p^\alpha}(n)$, where $\alpha \geq 2$, obtaining a simple proof of Salié's theorem.

2. **Three results.** Clearly in applying the above technique to $A_{p^\alpha}(n)$ we will need the number of incongruent solutions h modulo p^α of $h^2 - rh + 1 \equiv 0 \pmod{p^\alpha}$. Denoting this number by $N_{p^\alpha}(r)$ it is easily shown that for $\alpha \geq 2$ we have

$$(2.1) \quad N_{p^\alpha}(r) = \begin{cases} 1+(r^2-4 \mid p), & \text{if } r \not\equiv \pm 2 \pmod p, \\ \frac{1}{2}p^{\beta/2}(1+(s \mid p))(1+(-1)^\beta), & \text{if } r \equiv \pm 2 \pmod p, \\ & r \not\equiv \pm 2 \pmod{p^\alpha}, \\ \quad \text{say } r \equiv \pm 2 + p^\beta s, \text{ where } p \nmid s \text{ and } 1 \leq \beta \leq \alpha - 1, \\ p^{[\alpha/2]}, & \text{if } r \equiv \pm 2 \pmod{p^\alpha}. \end{cases}$$

Two well-known sums will also be needed. These are the Ramanujan sum (see for example [1])

$$(2.2) \qquad R_{p^\alpha}(n) = \sum_{h \bmod p^\alpha}{}' \exp(2\pi i n h/p^\alpha) = \begin{cases} -1, & \text{if } \alpha = 1, \\ 0, & \text{if } \alpha \geq 2, \end{cases}$$

and the Gauss sum (see for example [4])

$$(2.3) \quad G_{p^\alpha}(n) = \sum_{h \bmod p^\alpha}{}' (h \mid p) \exp(2\pi i n h/p^\alpha) = \begin{cases} (n \mid p) i^{(p-1)^2/4} p^{1/2}, & \text{if } \alpha \geq 1, \\ 0, & \text{if } \alpha \geq 2. \end{cases}$$

In each case when $\alpha \geq 2$ the result is easily proved by applying the bijection $h \to h+p$.

3. **Proof of theorem.** For $\alpha \geq 2$ we have

$$A_{p^\alpha}(n) = \sum_{h \bmod p^\alpha}{}' \exp(2\pi i n(h+\bar{h})/p^\alpha) = \sum_{r \bmod p^\alpha} \exp(2\pi i n r/p^\alpha) \sum_{\substack{h \bmod p^\alpha \\ h+\bar{h} \equiv r \pmod{p^\alpha}}}{}' 1,$$

that is

$$(3.1) \qquad A_{p^\alpha}(n) = \sum_{r \bmod p^\alpha} \exp(2\pi i n r/p^\alpha) N_{p^\alpha}(r).$$

By (2.1) the terms in (3.1) with $r \not\equiv \pm 2 \pmod p$ contribute

$$(3.2) \qquad \Sigma_1 = \sum_{r \bmod p^\alpha} \exp(2\pi i n r/p^\alpha)\{1+(r^2-4 \mid p)\}.$$

Setting $r = s + tp^{\alpha-1}$ in (3.2) we obtain

$$(3.3) \quad \Sigma_1 = \sum_{\substack{s \bmod p^{\alpha-1} \\ s \not\equiv \pm 2 \pmod p}} \exp(2\pi i n s/p^\alpha)\{1+(s^2-4 \mid p)\} \sum_{t \bmod p} \exp(2\pi i n t/p) = 0.$$

By (2.1) the terms in (3.1) with $r \equiv \pm 2 \pmod{p^\alpha}$ contribute

$$(3.4) \qquad \Sigma_2 = p^{[\alpha/2]}(\exp(4\pi i n/p^\alpha) + \exp(-4\pi i n/p^\alpha)).$$

Noting that $N_{p^\alpha}(r)=N_{p^\alpha}(-r)$ the terms in (3.1) with $r\equiv\pm 2(\operatorname{mod} p)$ and $r\not\equiv \pm 2(\operatorname{mod} p^\alpha)$ contribute

$$\begin{aligned}\Sigma_3 &= \sum_{\substack{r \bmod p^\alpha \\ r\equiv 2(\bmod p) \\ r\not\equiv 2(\bmod p^\alpha)}} \{\exp(2\pi inr/p^\alpha)+\exp(-2\pi inr/p^\alpha)\}N_{p^\alpha}(r) \\ &= \sum_{\substack{\beta=1 \\ \beta \text{ even}}}^{\alpha-1} \sideset{}{'}\sum_{s \bmod p^{\alpha-\beta}} \{\exp(2\pi in(2+p^\beta s)/p^\alpha) \\ &\qquad +\exp(-2\pi in(2+p^\beta s)/p^\alpha)\}p^{\beta/2}\{1+(s\mid p)\} \\ &= \sum_{\substack{\beta=1 \\ \beta \text{ even}}}^{\alpha-1} p^{\beta/2}\{\exp(4\pi in/p^\alpha)(R_{p^{\alpha-\beta}}(n)+G_{p^{\alpha-\beta}}(n)) \\ &\qquad +\exp(-4\pi in/p^\alpha)(R_{p^{\alpha-\beta}}(-n)+G_{p^{\alpha-\beta}}(-n))\},\end{aligned}$$

giving

$$\Sigma_3 = \begin{cases} 0, & \text{if } \alpha \text{ even}, \\ p^{(\alpha-1)/2}\{\exp(4\pi in/p^\alpha)(-1+(n\mid p)i^{(p-1)^2/4}p^{1/2}) \\ \qquad +\exp(-4\pi in/p^\alpha)(-1+(-n\mid p)i^{(p-1)^2/4}p^{1/2})\}, & \text{if } \alpha \text{ odd}, \end{cases} \tag{3.5}$$

since by (2.2) and (2.3) each Ramanujan and Gauss sum vanishes except when α is odd and $\beta=\alpha-1$. The theorem now follows from (3.3), (3.4) and (3.5) as

$$A_{p^\alpha}(n) = \Sigma_1+\Sigma_2+\Sigma_3.$$

References

1. G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, Oxford Univ. Press, London, (1962), p. 237.
2. H. Salié, *Uber die Kloostermanschen Summen $S(u, v; q)$*, Math. Z. **34** (1931), 91–109.
3. A. Weil, *On some exponential sums*, Proc. Nat. Acad. Sci. U.S.A. **34** (1948), 204–207.
4. A. L. Whiteman, *A note on Kloosterman sums*, Bull. Amer. Math. Soc., **51** (1945), 373–377.
5. K. S. Williams, *Note on the Kloosterman sum*, Proc. Amer. Math. Soc. **30** (1971), 61–62.

Carleton University,
Ottawa, Canada