# ON SALIÉ'S SUM

*by* L. J. MORDELL†

(Received 2 April, 1971)

Let $p$ be an odd prime and let $f(x)$ be a complex-valued function such that $f(x+p) = f(x)$ for all integers $x$. Write $e(x) = \exp(2\pi ix/p)$, and define $1/x$ by $\bar{x}$, where $x\bar{x} \equiv 1 \pmod{p}$. We consider the sum

$$S = \sum_{x=1}^{p-1} f\left(ax+\frac{b}{x}\right)\left(\frac{x}{p}\right) \quad \text{for} \quad ab \not\equiv 0 \pmod{p}, \tag{1}$$

where $\left(\frac{x}{p}\right)$ is the Legendre symbol. The sum is zero if $\left(\frac{ab}{p}\right) = -1$, as is clear on replacing $x$ by $b/ax$. Salié has found a result which can be written in the form

$$\sum_{x=1}^{p-1} e\left(ax+\frac{b}{x}\right)\left(\frac{x}{p}\right) = i^{\{\frac{1}{2}(p-1)\}^2}\left(\frac{a}{p}\right)p^{\frac{1}{2}}\{e(h)+e(-h)\}, \tag{2}$$

when $h^2 \equiv 4ab \pmod{p}$.

This permits of further applications, as I have shown **[1]** in a forthcoming paper. Recently, **[2]** K. S. Williams has found a result which can be written more symmetrically as

$$\sum_{x=1}^{p-1} f\left(x+\frac{1}{x}\right)\left(\frac{x}{p}\right) = \sum_{x=0}^{p-1} f(x)\left(\frac{x+2}{p}\right) + \sum_{x=0}^{p-1} f(x)\left(\frac{x-2}{p}\right). \tag{3}$$

If $h \not\equiv 0 \pmod{p}$, on making the substitution

$$x \to x/h, \quad f(x) \to f(hx),$$

(3) becomes

$$\sum_{x=1}^{p-1} f\left(x+\frac{h^2}{x}\right)\left(\frac{x}{p}\right) = \sum_{x=0}^{p-1} f(x)\left(\frac{x+2h}{p}\right) + \sum_{x=0}^{p-1} f(x)\left(\frac{x-2h}{p}\right). \tag{4}$$

Suppose now that $a$ and $b$ are two integers such that $\left(\frac{ab}{p}\right) = 1$. Define a value of $h$ by $h^2 \equiv ab \pmod{p}$. Replace $x$ by $ax$ on the left-hand side of (4). We then have

$$\left(\frac{a}{p}\right)\sum_{x=1}^{p-1} f\left(ax+\frac{b}{x}\right)\left(\frac{x}{p}\right) = \sum_{x=0}^{p-1} f(x)\left(\frac{x+2h}{p}\right) + \sum_{x=0}^{p-1} f(x)\left(\frac{x-2h}{p}\right), \tag{5}$$

a result of which Williams informs me he was aware.

Williams's proof of (3) is quite simple, but I give a different one. In (3), corresponding terms of the two series on the right-hand side cancel unless

$$\left(\frac{x+2}{p}\right)\left(\frac{x-2}{p}\right) = \left(\frac{x^2-4}{p}\right) = 1.$$

† Professor Mordell died on 12 March, 1972.

https://doi.org/10.1017/S0017089500001695 Published online by Cambridge University Press

On writing $x^2-4 \equiv (x-2t)^2 \pmod p$, this gives $x \equiv t+1/t$. The same value for $x$ occurs for two values of $t$ unless $x = \pm 2$, $t = \pm 1$. Hence

$$\tfrac{1}{2}\sum_{x\neq\pm 1} f\left(x+\frac{1}{x}\right)\left(\frac{x}{p}\right)+f(2)\left(\frac{1}{p}\right)+\tfrac{1}{2}\sum_{x\neq\pm 1} f\left(x+\frac{1}{x}\right)\left(\frac{x}{p}\right)+f(-2)\left(\frac{1}{p}\right)$$
$$=\sum_{x=0}^{p-1} f(x)\left(\frac{x+2}{p}\right)+\sum_{x=0}^{p-1} f(x)\left(\frac{x-2}{p}\right),$$

which is equivalent to (3).

Now put $f(x) = e(x)$, and replace $h$ by $\frac{1}{2}h$. Then the right-hand side of (5) becomes a gaussian sum; whence

$$\{e(h)+e(-h)\}\sum_{x=0}^{p-1} e(x)\left(\frac{x}{p}\right) = i^{\{\frac{1}{2}(p-1)\}^2}p^{\frac{1}{2}}\{e(h)+e(-h)\},$$

where $h^2 \equiv 4ab \pmod p$. This gives (2) in a slightly different form from that found by Williams.

## REFERENCES

**1.** L. J. Mordell, On some exponential sums related to Kloosterman sums, *Acta Arithmetica*; to appear.

**2.** K. S. Williams, On Salié's sum, *J. Number Theory* 3 (1971), 316–317.

ST. JOHN'S COLLEGE
CAMBRIDGE

https://doi.org/10.1017/S0017089500001695 Published online by Cambridge University Press