A NOTE ON GAUSS' SUM

L. CARLITZ

The formula

$$S = \sum_{r=0}^{p-1} e^{2\pi i r^2/p} = i^{(p-1)^2/4} p^{1/2}, \tag{1}$$

where p is an odd prime, has been proved in a variety of ways. In particular the proof in [3, p. 623] may be cited. We remark that Estermann [1] has recently given a simple proof of (1) that is valid for arbitrary odd p.

In the present note we indicate a short proof of (1) that makes use of some familiar results from cyclotomy. Let $\epsilon = e^{2\pi i/p}$ and let g denote a primitive root (mod p); define the determinant of order $p-1$

$$D = \left| \epsilon^{g^{r-s}} \right| \qquad (r, s = 0, 1, \cdots, p-2).$$

Then it is clear that D is also equal to the determinant

$$\Delta' = \left| \epsilon^{rs'} \right| \qquad (r, s = 1, 2, \cdots, p-1),$$

where $ss' \equiv 1 \pmod p$; this in turn is equal to

$$(-1)^{(p-3)/2}\Delta = (-1)^{(p-3)/2} \left| \epsilon^{rs} \right| \qquad (r, s = 1, 2, \cdots, p-1),$$

since it is necessary to make $(p-3)/2$ interchanges in going from Δ' to Δ. In the next place it is known [3, p. 465] that

$$\prod_{1 \leqq r < s < p} (\epsilon^r - \epsilon^s) = i^{(p-1)/2} p^{(p-2)/2}$$

and consequently

$$\Delta = (-1)^{(p-1)/2} i^{(p-1)/2} p^{(p-2)/2}.$$

This yields

$$D = - i^{(p-1)/2} p^{(p-2)/2}. \tag{2}$$

(We remark that (2) is stated incorrectly in [2, p. 479].)

Now on the other hand since D is a circulant we have also

$$D = \prod_{r=0}^{p-2} (\alpha^r, \epsilon), \tag{3}$$

where

Received by the editors October 7, 1955.

$$(\alpha^r, \epsilon) = \sum_{s=0}^{p-2} \alpha^{rs} \epsilon^{g^s} \qquad (\alpha = e^{2\pi i/(p-1)}).$$

But [3, p. 612] $(1, \epsilon) = -1$, $(\alpha^r, \epsilon)(\alpha^{-r}, \epsilon) = (-1)^r p$ and $(-1, \epsilon) = S$. Thus (3) becomes

$$D = -(-1)^{(p-1)(p-3)/8} p^{(p-3)/2} S. \tag{4}$$

Substituting from (4) in (2) we immediately get (1).

References

1. T. Estermann, *On the sign of the Gaussian sum*, J. London Math. Soc. vol. 20 (1945) pp. 66–67.
2. T. Muir and W. H. Metzler, *Theory of determinants*, New York, 1933.
3. H. Weber, *Algebra*, vol. 1, 2d. ed., Braunschweig, 1898.

Duke University