The formula

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

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 \( e = e^{2\pi i/p} \) and let \( g \) denote a primitive root \((\text{mod} \ p)\); define the determinant of order \( p-1 \)

\[ D = \left| e^{rs} \right| \quad (r, s = 0, 1, \ldots, p - 2). \]

Then it is clear that \( D \) is also equal to the determinant

\[ \Delta' = \left| e^{rs'} \right| \quad (r, s = 1, 2, \ldots, p - 1), \]

where \( ss' \equiv 1 \pmod{p} \); this in turn is equal to

\[ (-1)^{(p-3)/2} \Delta = (-1)^{(p-3)/2} \left| e^{rs} \right| \quad (r, s = 1, 2, \ldots, p - 1), \]

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

\[ \prod_{1 \leq r < s < p} (e^r - e^s) = i^{(p-1)/2} p^{(p-2)/2} \]

and consequently

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

This yields

\[ D = - i^{(p-1)/2} p^{(p-2)/2}. \]

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

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

\[ D = \prod_{r=0}^{p-2} (\alpha^r, \epsilon), \]

where

Received by the editors October 7, 1955.
A NOTE ON GAUSS' SUM

\[ (\alpha^r, e) = \sum_{s=0}^{p-2} \alpha^{rs} e^s \] (\alpha = e^{2\pi i/(p-1)}).

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

\[ (4) \quad D = -(-1)^{(p-1)(p-8)/8} p^{(p-4)/2} S.\]

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

REFERENCES


Duke University