THE SIGN OF THE GAUSSIAN SUM

Dedicated to Hans Rademacher
on the occasion of his seventieth birthday

BY
L. J. MORDELL

It is well known and easily proved that if p is an odd prime, then

$$\sum_{s=0}^{p-1} e^{2\pi i s^2/p} = c\sqrt{p}, \tag{1}$$

where $c = \pm 1$ if $p \equiv 1 \pmod 4$ and $c = \pm i$ if $p \equiv 3 \pmod 4$. (See, for example, the remark on Theorem 212 in Landau's *Vorlesungen über Zahlentheorie*.) As Gauss noted many years ago, it is a much more difficult matter to show that the plus sign must be taken in both cases. A proof originating from Kronecker is given by Hasse in his *Vorlesungen über Zahlentheorie* (pp. 449–452). It may be worthwhile to give a proof not very dissimilar from this but perhaps a trifle simpler and more self-contained.

Write

$$\zeta = e^{2\pi i/p}, \qquad P = \zeta - 1.$$

Then from the identity

$$x^{p-1} + x^{p-2} + \cdots + x + 1 = \prod_{n=1}^{p-1} (x - \zeta^n)$$

and the equalities

$$(1 - \zeta^n)/(1 - \zeta) = 1 + \zeta + \zeta^2 + \cdots + \zeta^{n-1},$$
$$(1 - \zeta)/(1 - \zeta^n) = 1 + \zeta^n + \zeta^{2n} + \cdots + \zeta^{(m-1)n},$$

where $mn \equiv 1 \pmod p$, we have

$$p = \prod_{n=1}^{p-1} (1 - \zeta^n) = \varepsilon P^{p-1}, \tag{2}$$

where ε is a unit. We prove further that

$$\sqrt{p} = \prod_{n=1}^{(p-1)/2} \{2 \sin (2n\pi/p)\}. \tag{3}$$

In fact from the identity

$$x^{p-1} + x^{p-2} + \cdots + x + 1 = \prod_{n=1}^{(p-1)/2} (x - \zeta^{2n})(x - \zeta^{-2n}),$$

we have

$$\begin{aligned} p &= \prod_{n=1}^{(p-1)/2} (1 - \zeta^{2n})(1 - \zeta^{-2n}) \\ &= \prod_{n=1}^{(p-1)/2} (\zeta^{-n} - \zeta^n)(\zeta^n - \zeta^{-n}) \\ &= \prod_{n=1}^{(p-1)/2} \{2 \sin (2n\pi/p)\}^2, \end{aligned}$$

from which (3) follows, since each sine is positive.

Received June 1, 1961.

Now (1) may be written

$$c\sqrt{p} = \sum_{s=0}^{p-1} \zeta^{s^2} = \sum_r \zeta^r = \sum_r (1+P)^r,$$

where $r \equiv s^2 \pmod p$ and $0 \leqq r < p$. But

$$\sum_r (1+P)^r = \sum_r \left\{1 + \sum_{t=1}^{p-1} \frac{r(r-1)\cdots(r-t+1)}{t!} P^t\right\},$$

the summand in the inner sum being zero when $t > r$. Since

$$\sum_r r^a \equiv \sum_{s=0}^{p-1} s^{2a} \equiv \begin{cases} 0 \pmod p & \text{if } 0 < a < p-1,\ a \neq (p-1)/2, \\ -1 \pmod p & \text{if } a = (p-1)/2, \end{cases}$$

and since $p \equiv 0 \pmod{P^{(p+1)/2}}$, we have

$$\{(p-1)/2\}! \sum_r (1+P)^r \equiv -P^{(p-1)/2} \pmod{P^{(p+1)/2}}.$$

Thus,

$$\{(p-1)/2\}!\, c\sqrt{p} \equiv -P^{(p-1)/2} \pmod{P^{(p+1)/2}}. \tag{4}$$

Now by (3)

$$\sqrt{p} = (-i)^{(p-1)/2} \prod_{n=1}^{(p-1)/2} (\zeta^n - \zeta^{-n}).$$

But $\zeta^n \equiv 1 + nP \pmod{P^2}$ and $\zeta^{-n} \equiv 1 - nP \pmod{P^2}$, so that

$$\sqrt{p} \equiv (-2i)^{(p-1)/2} \{(p-1)/2\}!\, P^{(p-1)/2} \pmod{P^{(p+1)/2}}. \tag{5}$$

Comparing (4) and (5), we obtain

$$-1 \equiv (-2i)^{(p-1)/2} (\{(p-1)/2\}!)^2 c \pmod P.$$

Since both sides here are rational integers, this last congruence also holds modulo p. By Wilson's theorem

$$(\{(p-1)/2\}!)^2 \equiv (-1)^{(p+1)/2} \pmod p,$$

so that we have

$$1 \equiv 2^{(p-1)/2}\, i^{(p-1)/2} c \pmod p. \tag{6}$$

Suppose first that $p \equiv 1 \pmod 4$. In this case

$$2^{(p-1)/2} \equiv \left(\frac{2}{p}\right) \equiv (-1)^{(p-1)/4} \pmod p.$$

Hence (6) gives $1 \equiv c \pmod p$, and thus $c = 1$.

Suppose next that $p \equiv 3 \pmod 4$. In this case

$$2^{(p-1)/2} \equiv \left(\frac{2}{p}\right) \equiv (-1)^{(p+1)/4} \pmod p.$$

Hence (6) gives $1 \equiv -ic \pmod p$, and thus $c = i$.

Addendum (August 6, 1961). Professor Bateman remarks to me that the only part of the above proof depending upon analysis is the argument showing

that the identity

$$\sqrt{p} = \pm \prod_{n=1}^{(p-1)/2} \left(\frac{\zeta^n - \zeta^{-n}}{i} \right), \qquad \zeta = e^{2\pi i/p},$$

requires the positive sign. This is of course trivial, since

$$\zeta^n - \zeta^{-n} = 2i \sin(2n\pi/p).$$

Hasse in his proof similarly remarks that it uses only the fact that the sign of $\sin(\pi x + \pi x/p)$ for $x = 1, 2, \cdots, (p-1)/2$ is alternately negative and positive. It seems of interest to free the proof from analysis (specifically, the properties of the sine and exponential functions), and this is now done. The value of ζ must be defined as that complex p^{th} root of unity with greatest real part and also with positive imaginary part, so that $(\zeta - \zeta^{-1})/i = (\zeta - \bar{\zeta})/i > 0$.

We have to prove that

$$(\zeta^n - \zeta^{-n})/i > 0 \quad (n = 1, 2, \cdots, (p-1)/2),$$

i.e., that $f_n(\zeta) > 0$ for $n = 1, 2, \cdots, (p-1)/2$, where

$$f_n(z) = (z^n - z^{-n})/(z - z^{-1}) = z^{n-1} + z^{n-3} + \cdots + z^{-n+1}.$$

Write $K = z + z^{-1}$ and $f_n(z) = g_n(K)$, so that

$$g_{n+1}(K) - Kg_n(K) + g_{n-1}(K) = 0,$$

$$g_1(K) = 1, \quad g_2(K) = K, \quad g_3(K) = K^2 - 1, \quad g_4(K) = K^3 - 2K, \quad \cdots,$$

and $g_n(K)$ is a polynomial in K of degree $n - 1$ with leading term K^{n-1}. Clearly no two consecutive g's can vanish simultaneously, and, if g_n vanishes at some point, then g_{n+1} and g_{n-1} take values of opposite signs there.

Write

$$g(K) = g_{(p-1)/2}(K) + g_{(p+1)/2}(K),$$

so that $g(K)$ is a polynomial in K of degree $(p-1)/2$ with leading term $K^{(p-1)/2}$. On substituting we find

$$g(K) = (z^{p-1} + z^{p-2} + \cdots + 1)/z^{(p-1)/2}.$$

Hence the roots of $g(K) = 0$ are given by

$$K = \zeta^n + \zeta^{-n} \qquad \text{for } n = 1, 2, \cdots, (p-1)/2;$$

and $\lambda = \zeta + \zeta^{-1}$ is the greatest root. Let $\lambda_2, \lambda_3, \cdots$ be the greatest real roots of the equations $g_2(K) = 0, g_3(K) = 0, \cdots$ respectively. We first prove that these exist and that $\lambda_{n-1} < \lambda_n$ for $n = 3, 4, \cdots, (p-1)/2$. We then prove that $\lambda > \lambda_{(p-1)/2}$, and this shows at once that

$$f_n(\zeta) = g_n(\lambda) > 0 \quad (n = 1, 2, \cdots, (p-1)/2).$$

To prove the first assertion we begin by noting that λ_2 and λ_3 exist and $\lambda_2 < \lambda_3$. Now assume that $2 < n < (p-1)/2$ and that $\lambda_2, \cdots, \lambda_n$ exist

with $\lambda_2 < \cdots < \lambda_{n-1} < \lambda_n$. Since $g_n(\lambda_n) = 0$ and since λ_{n-1} is the greatest root of $g_{n-1}(K) = 0$, we have

$$g_{n+1}(\lambda_n) = -g_{n-1}(\lambda_n) < 0.$$

Hence $g_{n+1}(K) = 0$ has a root greater than λ_n. Thus λ_{n+1} exists and $\lambda_{n+1} > \lambda_n$.

To prove the second assertion write $m = (p+1)/2$, $\lambda' = \lambda_{(p-1)/2}$. Then

$$g(\lambda') = g_m(\lambda') < 0,$$

since

$$g_m(\lambda') - \lambda' g_{m-1}(\lambda') + g_{m-2}(\lambda') = 0,$$

where $g_{m-1}(\lambda') = 0$ and $g_{m-2}(\lambda') > 0$. Thus $g(K) = 0$ has a root greater than λ', i.e., $\lambda > \lambda'$.

This finishes the desired proof

UNIVERSITY OF NOTRE DAME
NOTRE DAME, INDIANA
ST. JOHN'S COLLEGE
CAMBRIDGE, ENGLAND