A THEOREM ON QUADRATIC RESIDUES

LEO MOSER

We give a short proof of the following result.

THEOREM. *For every prime* $p \equiv 3 \pmod 4$,

$$E = \sum_{h=1}^{(p-1)/2} \left(\frac{h}{p}\right) > 0,$$

that is, the number of quadratic residues in the range 0 *to* $(p-1)/2$ *exceeds the number of nonresidues in this range.*

This theorem seems to have been first conjectured by Jacobi and proved by Dirichlet [**1**][1] in connection with the theory of binary quadratic forms. Proofs are also given in the books of Bachmann [**2**] and Landau [**3**]. More recent proofs are due to Kai-Lai Chung [**4**] and A. L. Whiteman [**5**]. All known proofs, including the one given here, are analytic. While a really elementary proof would be of great interest, the following proof may merit consideration because of its brevity.

Our starting point is the following Gaussian summation, proved in [**3**].

$$\sum_{r=1}^{p-1} \left(\frac{r}{p}\right) e^{2\pi i r/p} = i(p)^{1/2}. \tag{1}$$

By taking imaginary parts, making the substitution $r = n \cdot h$, and multiplying through by

$$\frac{1}{p^{1/2} \cdot n} \left(\frac{n}{p}\right)$$

in (1) we obtain

$$\frac{1}{n}\left(\frac{n}{p}\right) = \frac{1}{p^{1/2}} \sum_{h=1}^{p-1} \left(\frac{h}{p}\right) \frac{\sin(2\pi n h/p)}{n}. \tag{2}$$

Summing (2) over odd n we get

$$\sum_{m=1}^{\infty} \frac{1}{(2m-1)} \left(\frac{2m-1}{p}\right) = \frac{1}{p^{1/2}} \sum_{h=1}^{p-1} \left(\frac{h}{p}\right) \sum_{m=1}^{\infty} \frac{\sin(2\pi(2m-1)h/p)}{2m-1}. \tag{3}$$

Now by a well known Fourier expansion

Received by the editors June 30, 1950.

[1] Numbers in brackets refer to the references at the end of the paper.

$$\sum_{m=1}^{\infty} \frac{\sin (2m-1)\theta}{2m-1} = \begin{cases} \pi/4 & \text{for } 0 < \theta < \pi, \\ -\pi/4 & \text{for } \pi < \theta < 2\pi. \end{cases} \tag{4}$$

Using (4) in the right-hand side of (3) we obtain

$$\sum_{m=1}^{\infty} \frac{1}{2m-1}\left(\frac{2m-1}{p}\right) = \frac{\pi}{4p^{1/2}}\left[\sum_{h=1}^{(p-1)/2}\left(\frac{h}{p}\right) - \sum_{h=(p+1)/2}^{p-1}\left(\frac{h}{p}\right)\right]. \tag{5}$$

Now since -1 is a nonresidue of p,

$$\left(\frac{p-h}{p}\right) = -\left(\frac{h}{p}\right)$$

so that the bracket in (5) reduces to $2E$. Hence

$$\sum_{m=1}^{\infty} \frac{1}{(2m-1)}\left(\frac{2m-1}{p}\right) = \frac{\pi E}{2p^{1/2}}. \tag{6}$$

Now E is the difference of two integers whose sum is odd. Hence $E \neq 0$, and to prove $E > 0$ it suffices to show $E \geqq 0$. This we shall do by showing that the left-hand side of (7) is not negative.

Consider the following identity, valid for $s > 1$:

$$\sum_{m=1}^{\infty} \frac{1}{(2m-1)^s}\left(\frac{2m-1}{p}\right) = \prod_q \left(1 - \frac{1}{q^s}\left(\frac{q}{p}\right)\right)^{-1} \tag{7}$$

where q runs over all odd primes. The series on the left is uniformly convergent for $s \geqq 1$. Hence its sum is continuous at $s = 1$. The infinite product is clearly positive for $s > 1$. Hence the proof is complete.

It may be noted that the advantage of this proof is due mainly to the use of the Fourier series $\sum_{m=1}^{\infty} (\sin (2m-1)\theta/(2m-1))$ instead of $\sum_{m=1}^{\infty} (\sin m\theta/m)$. For class-number theory, the latter is the natural one, while for the purpose of just proving this theorem alone, the former achieves the desired goal more quickly.

References

1. L. Dirichlet, *Vorlesungen über Zahlentheorie*, 4th ed., §5.
2. P. Bachmann, *Analytische Zahlentheorie* II, §8.
3. E. Landau, *Vorlesungen über Zahlentheorie*, vol. 1, part 4, chap. 6.
4. Kai-Lai Chung, *Note on a theorem on quadratic residues*, Bull. Amer. Math. Soc. vol. 47 (1941) pp. 514–516.
5. A. L. Whiteman, *Theorems on quadratic residues*, Mathematics Magazine vol. 23 (1949) pp. 71–74.

Texas Technological College