Canad. Math. Bull. Vol. **26** (1), 1983

ON THE QUADRATIC RESIDUES (MOD p) IN THE INTERVAL $(0, p/4)$

BY

KENNETH S. WILLIAMS*

ABSTRACT. A short proof is given of a result of Burde giving the parity of the number of quadratic residues (mod p) in the interval $(0, p/4)$, where $p \equiv 1 (\bmod 4)$ is prime.

Let $p \equiv 1(\bmod 4)$ be a prime. We define (unique) integers a and b by

$$(1) \qquad p = a^2 + b^2, \qquad a \equiv 1(\bmod 4), \qquad b \equiv \left(\frac{p-1}{2}\right)!\, a(\bmod p).$$

Clearly we have

$$(2)(\mathrm{i}) \qquad p \equiv 2a - 1(\bmod 16), \qquad b \equiv 0(\bmod 4), \quad \text{if} \quad p \equiv 1(\bmod 8),$$

and

$$(2)(\mathrm{ii}) \qquad p \equiv 2a + 3(\bmod 16), \qquad b \equiv (\bmod 4), \quad \text{if} \quad p \equiv 5(\bmod 8).$$

Let $N(p)$ denote the number of quadratic residues (mod p) in the interval $(0, p/4)$. Burde [2: Theorems 1 and 2] has shown (with slightly different notation) that

$$(3)(\mathrm{i}) \qquad N(p) \equiv 0(\bmod 2) \Leftrightarrow b \equiv 0(\bmod 8), \quad \text{if} \quad p \equiv 1(\bmod 8),$$

and

$$(3)(\mathrm{ii}) \qquad N(p) \equiv 0(\bmod 2) \Leftrightarrow b \equiv 6(\bmod 8), \quad \text{if} \quad p \equiv 5(\bmod 8).$$

We give a very short proof of this result. We have

$$(4) \qquad N(p) = \tfrac{1}{2} \sum_{0<k<p/4} \left(1 + \left(\frac{k}{p}\right)\right).$$

Now, by a result of Dirichlet [4: p. 152] (or see [3: p. 101]), we have

$$(5) \qquad \sum_{0<k<p/4} \left(\frac{k}{p}\right) = \tfrac{1}{2} h(-4p),$$

Received by the editors October 13, 1981 and in revised form January 8, 1982.

AMS Subject Classification (1980): Primary 10A15; Secondary 10E15, 12H50, 12H25.

Research supported by Natural Sciences and Engineering Research Council Canada Grant A07233.

where $h(-4p)$ denotes the class number of the imaginary quadratic field $Q(\sqrt{-p})$ (of discriminant $-4p$). Hence, by (4) and (5), we have

$$8N(p) = p - 1 + 2h(-4p). \tag{6}$$

Now Gauss [5: p. 380] (see also Yamamoto [6: Lemma 3], Barkan [1: p. 828]) (Note: Gauss's k is related to $h(-4p)$ by $2k = h(-4p)$.) has shown that

$$h(-4p) \equiv -a + b + 1 \pmod 8, \tag{7}$$

so by (6) and (7) we have

$$8N(p) \equiv p - 2a + 2b + 1 \pmod{16}. \tag{8}$$

Hence, from (2) and (8), we obtain

$$4N(p) \equiv \begin{cases} b \pmod 8, & \text{if } p \equiv 1 \pmod 8, \\ b + 2 \pmod 8, & \text{if } p \equiv 5 \pmod 8, \end{cases}$$

which completes the proof of Burde's result.

REFERENCES

1. Philippe Barkan, Une propriété de congruence de la longueur de la periode d'un developpement en fraction continue, *C.R. Acad. Sc. Paris* **281** (1975), 825–828.

2. Klaus Burde, Eine Verteilungseigenschaft der Legendresymbole, *J. Number Theory* **12** (1980), 273–277.

3. L. E. Dickson, History of the Theory of Numbers, Volume 3, reprinted Chelsea Publishing Company, Bronx, N.Y. (1966).

4. P. G. L. Dirichlet, Recherches sur diverses applications de l'analyse infinitésimale à la théorie des nombres, *J. Reine Angew. Math.* **21** (1840), 134–155.

5. Carl Friedrich Gauss, Letter to P. G. L. Dirichlet dated 30 May 1828. (Reproduced in G. Lejeune Dirichlet's Werke, Chelsea Publishing Company, Bronx, N.Y. (1969) Volume 2, pp. 378–380.)

6. Koichi Yamamoto, On Gaussian sums with biquadratic residue characters, *J. Reine Angew. Math.* **219** (1965), 200–213.

DEPARTMENT OF MATHEMATICS AND STATISTICS
CARLETON UNIVERSITY
OTTAWA, ONTARIO, CANADA, K1S 5B6