A NOTE ON POWER RESIDUES

By L. Carlitz

If p is a prime $\equiv 1 \pmod 4$, $h = h(p)$ the class number of the real quadratic field $R(p^{\frac{1}{2}})$ and $\epsilon = (t + up^{\frac{1}{2}})/2$ the fundamental unit of the field ($\epsilon > 1$), Ankeny, Artin and Chowla [1] have stated the following result:

$$2uh/t \equiv (A + B)/p \pmod p, \tag{1}$$

where A is the product of the quadratic residues of p and B is the product of the non-residues in the interval $1, p - 1$. In [2] it is shown that (1) is a consequence of

$$uh/t \equiv B_{\frac{1}{2}(p-1)} \pmod p \tag{2}$$

and

$$\frac{1}{p}(A + B) \equiv 2B_{\frac{1}{2}(p-1)} \pmod p; \tag{3}$$

here B_m denotes a Bernoulli number in the even suffix notation.

In view of the above it may be of interest to consider the following problem. Let $p = km + 1$ denote a prime, $k > 1$, $m > 1$, and g a primitive root $\pmod p$. The numbers $1, \cdots, p - 1$ are separated into k classes $C_0, \cdots, C_{k-1}$ each containing m numbers in the following manner. The number $a \in C_i$ provided

$$a \equiv g^{ks+i} \pmod p \tag{4}$$

for some s. We then put

$$A_i = \prod_{a \in C_i} a \qquad (i = 0, 1, \cdots, k - 1) \tag{5}$$

We also put

$$g^m \equiv w \pmod p \tag{6}$$

Now it follows from (4), (5) and (6) that

$$A_i \equiv \prod_{s=0}^{m-1} g^{ks+i} \equiv g^{\frac{1}{2}km(m-1)+mi} \equiv (-1)^{m-1}w^i \pmod p$$

We next put (compare [3; Chapter 19])

$$(-1)^m w^{-i} A_i = -1 + p\Omega_i, \tag{7}$$

where Ω_i is integral $\pmod p$. Hence defining the Fermat quotient $q(r)$ by means of

$$q(r) = \frac{r^{p-1} - 1}{p} \qquad (p \nmid r), \tag{8}$$

Received May 5, 1955.