A THEOREM OF BREWER ON CHARACTER SUMS

Dedicated to Professor H. S. Vandiver on his eightieth birthday.

By Albert Leon Whiteman

1. **Introduction.** It is well known that an odd prime p can be represented uniquely in the form $c^2 + 2d^2$ if and only if $p = 8k + 1$ or $p = 8k + 3$. In a recent paper Brewer [1] has expressed c in terms of the sum

$$B = \sum_{u=0}^{p-1} \chi((u+2)(u^2-2)), \tag{1.1}$$

where $\chi(n)$ is the quadratic character of n modulo p. His precise result may be stated as follows.

Theorem. *The sum B satisfies*

$$B = \begin{cases} 0 & (p \neq c^2 + 2d^2), \\ 2c & (p = c^2 + 2d^2), \end{cases}$$

the sign of c being determined by the condition $c \equiv (-1)^{k+1} \pmod 4$.

Brewer's method of proof makes essential use of the following congruences. If $p = c^2 + 2d^2 (c \equiv (-1)^{k+1} \pmod 4)$, then

$$2c \equiv \begin{cases} -\binom{4k}{k} \pmod p & (p = 8k+1), \\ \binom{4k+1}{k} \pmod p & (p = 8k+3). \end{cases} \tag{1.2}$$

The first congruence in (1.2) is due to Stern [4]; the second is due to Eisenstein [2]. Brewer remarks that it would be of interest to prove his theorem without employing these congruences.

The purpose of this paper is to give a straightforward proof of the theorem from which (1.2) follows easily as a corollary.

2. **A preliminary lemma.** Let p be an odd prime and let γ denote a generator of the multiplicative group of the finite field $GF(p^2)$. For $\xi \in GF(p^2)$ put

$$\operatorname{tr}(\xi) = \xi + \xi^p, \tag{2.1}$$

so that $\operatorname{tr}(\xi) \in GF(p)$. If $\xi \neq 0$ let $\bar{\xi}$ be the unique solution of the equation

Received October 5, 1962. This research was partially supported by National Science Foundation grant G 9668. Presented to the Society, November 17, 1962.