THEOREMS ANALOGOUS TO JACOBSTAHL'S THEOREM

By Albert Leon Whiteman

1. **Introduction.** In his 1906 dissertation [4] Jacobstahl proved the theorem that if $p = 4f + 1 = a^2 + b^2$ is a prime, then $a = \frac{1}{2}\phi_2(r)$, $b = \frac{1}{2}\phi_2(n)$, $\frac{1}{2}\phi_2(-1) \equiv (p - 3)/2 \pmod 8$, where

$$\phi_q(s) = \sum_{m=0}^{p-1} (m/p)((m^q + s)/p), \tag{1.1}$$

and where r is any quadratic residue of p and n is any non-residue. The symbol (m/p) denotes the Legendre symbol. An analogous result (Theorem 3 of this paper) for $p = 3f + 1$ was obtained by L. von Schrutka [7] in 1911 and rediscovered by Chowla [2] in 1945.

The main purpose of this paper is to employ the powerful method of cyclotomy to derive a number of theorems of the Jacobstahl type for primes $p = ef + 1$. In particular, the case $e = 8$ is treated in §5 and the case $e = 5$ is treated in §7. The method of Jacobstahl and von Schrutka consists in ingenious verifications of certain identities taken over sums of quadratic characters, whereas the method of Chowla is based upon a theorem of Libri [6] on the number of solutions of a cubic congruence.

It may be remarked that our method serves for further values of e. However, we shall not go into this question in the present paper.

2. **Notation and preliminaries.** We shall follow the notation employed by Dickson [3] in his fundamental paper on cyclotomy. Let g be a primitive root of a prime p. Let e be a divisor of $p - 1$ and write $p - 1 = ef$. A number N, prime to p, is congruent to a power of g: $N \equiv g^{ez+h} \pmod p$, $0 \leq z \leq f - 1$, $0 \leq h \leq e - 1$. For fixed h and k, $0 \leq h, k \leq e - 1$, let (h, k) denote the number of sets of values of t and z, each chosen from $0, 1, \cdots, f - 1$ for which the congruence $g^{ez+h} \equiv 1 + g^{et+k} \pmod p$ holds.

The cyclotomic numbers (h, k) satisfy the following easily established properties (see [3; formulas (14), (15) and (17)])

$$(k, h) = (h, k) = (e - k, h - k) \qquad (f \text{ even}), \tag{2.1}$$

$$(k, h) = (h + \tfrac{1}{2}e, k + \tfrac{1}{2}e) = (e - k, h - k) \qquad (f \text{ odd}), \tag{2.2}$$

$$\sum_{h=0}^{e-1} (k, h) = f - n_k \qquad (k = 0, 1, \cdots, e - 1), \tag{2.3}$$

Received April 18, 1949.