1. Introduction. Let $k$ denote a fixed positive integer. A completely multiplicative arithmetical function $\chi$ is called a character modulo $k$ if $\chi$ is periodic with period $k$ and has the property that $\chi(n) = 0$ if and only if $(n, k) > 1$. It is well known that there are exactly $\phi(k)$ distinct characters modulo $k$ and that they form a multiplicative group, the identity element being the principal character $\chi_1$, where $\chi_1(n) = 1$ if $(n, k) = 1$. Here $\phi(k)$ is Euler’s totient.

A positive divisor $d$ of $k$ is called an induced modulus for $\chi$ if we have

$$\chi(n) = 1 \quad \text{whenever} \quad (n, k) = 1 \quad \text{and} \quad n \equiv 1 \pmod{d}. \quad (1)$$

This implies that $\chi$ is also a character modulo $d$. In particular, $k$ itself is always an induced modulus for $\chi$. The smallest induced modulus is called the conductor of $\chi$. A character $\chi$ modulo $k$ is called primitive if its conductor is $k$, that is, if it has no induced modulus less than $k$.

For any character $\chi$ modulo $k$ and any integer $r$ we consider the Gauss sum $G(r, \chi)$ defined by the equation

$$G(r, \chi) = \sum_{h \mod k} \chi(h)e^{2\pi i rh/k}, \quad (2)$$

where the sum is extended over any complete residue system modulo $k$. We call the Gauss sum separable if we have

$$G(r, \chi) = \tilde{\chi}(r)G(1, \chi). \quad (3)$$

It is well known that the Gauss sum $G(r, \chi)$ is separable if $\chi$ is a primitive character (see Lemma 3 below). This paper proves the converse. That is, if $G(r, \chi)$ is separable for every $r$, then $\chi$ is primitive. Therefore, we have the following alternate description of primitive characters.

**Theorem 1.** A character $\chi$ modulo $k$ is primitive if, and only if, the Gauss sum $G(r, \chi)$ is separable for every $r$.

2. Lemmas. The proof of Theorem 1 is based on seven lemmas. Lemma 6 describes a property of the Euler $\phi$-function which is crucial to the proof of Theorem 1 and also has applications elsewhere [1], [3, p. 24], [5, p. 66]. The other lemmas deal with characters and Gauss sums.

Received by the editors June 11, 1969.
Lemma 1. For any character \( \chi \) modulo \( k \), the Gauss sum \( G(r, \chi) \) is separable whenever \( (r, k) = 1 \).

Proof. Since \( (r, k) = 1 \) the numbers \( rh \) run through a complete residue system modulo \( k \) with \( h \). Also, \( |\chi(r)| = 1 \) so we have \( \chi(h) = \tilde{\chi}(r)\chi(r)\chi(h) = \tilde{\chi}(r)\chi(rh) \). Hence we can write

\[
G(r, \chi) = \sum_{h \mod k} \chi(h)e^{2\pi i rh/k} = \tilde{\chi}(r) \sum_{h \mod k} \chi(rh)e^{2\pi i rh/k}
\]

\[
= \tilde{\chi}(r) \sum_{m \mod k} \chi(m)e^{2\pi im/k} = \tilde{\chi}(r)G(1, \chi).
\]

This proves that \( G(r, \chi) \) is separable.

Lemma 2. Assume \( (r, k) > 1 \). Then \( G(r, \chi) \) is separable if and only if \( G(r, \chi) = 0 \).

Proof. If \( (r, k) > 1 \) we have \( \chi(r) \neq 0 \) so equation (3) holds if and only if \( G(r, \chi) = 0 \).

Lemma 3. If \( \chi \) is a primitive character modulo \( k \), then the Gauss sum \( G(r, \chi) \) is separable for every \( r \).

Proof. A proof of Lemma 3 is given in [2, Theorem 4.12, p. 312] and in [4, Lemma 1.1, p. 212].

Lemma 3, together with its converse (Lemma 7 below) give us Theorem 1. The next three lemmas are used to prove Lemma 7.

Lemma 4. If \( \chi \) is a primitive character mod \( k \), then \( |G(1, \chi)|^2 = k \).

Proof. A proof of Lemma 4 is given in [2, Theorem 4.13, p. 313] and in [4, Lemma 1.1, p. 212].

Lemma 5. Let \( \chi \) be any character modulo \( k \) and let \( d \) be the conductor of \( \chi \). Then there exists a primitive character \( \psi \) modulo \( d \) such that

\[
\chi(n) = \psi(n)\chi_1(n),
\]

where \( \chi_1 \) is the principal character modulo \( k \).

Proof. We define \( \psi(n) \) by the equation \( \psi(n) = \chi(n)/\chi_1(n) \) if \( (n, d) = 1 \) and we let \( \psi(n) = 0 \) if \( (n, d) > 1 \). Then equation (4) holds for all \( n \). It is easy to verify that \( \psi \) is a character modulo \( d \). To prove that \( \psi \) is a primitive character modulo \( d \), let \( q \) be any induced modulus for \( \psi \). Then we have

\[
\psi(n) = 1 \quad \text{if} \quad (n, d) = 1 \quad \text{and} \quad n \equiv 1 \pmod{q}.
\]

Equation (4) implies that \( \chi(n) = 1 \) if \( (n, k) = 1 \) and \( n \equiv 1 \pmod{q} \), so \( q \) is also an induced modulus for \( \chi \). Hence \( q \geq d \) since \( d \) is the conductor.
of \( \chi \). Therefore the conductor of \( \psi \) is equal to \( d \) so \( \psi \) is primitive modulo \( d \). This proves Lemma 5.

The next lemma concerns decomposition of reduced residue systems.

**Lemma 6.** Let \( S_k \) denote a reduced residue system modulo \( k \), and let \( d \) be a divisor of \( k \). Then \( S_k \) is the union of \( \phi(k) / \phi(d) \) disjoint sets, each of which is a reduced residue system modulo \( d \).

**Proof.** Consider \( S_k \) as a multiplicative group of reduced residue classes modulo \( k \), and let \( S_d \) be the group of reduced residue classes modulo \( d \). Let the classes of \( S_k \) be represented by integers \( n \) and those of \( S_d \) by integers \( r \), and note that each \( n \) is congruent (mod \( d \)) to a number \( r \) since \( d | k \). Define a mapping \( f: S_k \to S_d \) as follows:

If \( n \in S_k \), then \( f(n) = r \), where \( n \equiv r \) (mod \( d \)).

This mapping is a homomorphism of \( S_k \) into \( S_d \). The homomorphism is onto because if \( (r, d) = 1 \) there always exists an integer \( n \) such that

\[ n \equiv r \pmod{d} \quad \text{and} \quad (n, k) = 1. \]

In fact, we can take for \( n \) the solution to the system of congruences

\[ x \equiv r \pmod{d}, \quad x \equiv 1 \pmod{k'}, \]

where \( k' \) is the product of those prime factors of \( k \) which do not divide \( d \). Since \( (k', d) = 1 \) this system has a solution (by the Chinese remainder theorem). To prove that \( (n, k') = 1 \) we note that \( (n, k') = 1 \) because \( n \equiv 1 \) (mod \( k' \)) and that \( (n, d) = 1 \) because \( n \equiv r \) (mod \( d \)). Hence \( (n, k'd) = 1 \). But \( k \) and \( k'd \) have the same set of prime factors, so \( (n, k) = 1 \).

Now let \( K \) be the kernel of \( f \), that is, \( K = \{ x \in S_k | x \equiv 1 \pmod{d} \} \). Then the factor group \( S_k/K \) is isomorphic to the group \( S_d \), so we have a corresponding coset decomposition

\[ S_k = \bigcup_{x \in T} xK, \]

where \( T \) is a set of coset representatives. If we take one representative from each coset we get a reduced residue system modulo \( d \). There are \( \phi(k) \) elements in \( S_k \) and \( \phi(d) \) elements in each reduced residue system modulo \( d \), so there are \( \phi(k) / \phi(d) \) such residue systems altogether. This completes the proof of Lemma 6.

**Note.** The referee has pointed out that Lemma 6 was proved in 1923 by T. Nagell [3], and that a different proof was later given by R. Vaidyanathaswamy [5]. Our group-theoretic proof is different from each of these.
Now we use Lemmas 4, 5, and 6 to prove the converse of Lemma 3.

**Lemma 7.** If a character \( \chi \) modulo \( k \) has separable Gauss sums \( G(r, \chi) \) for every \( r \), then \( \chi \) is primitive modulo \( k \).

**Proof.** Because of Lemmas 1 and 2, it suffices to prove that if \( \chi \) is not primitive then for some \( r \) satisfying \( (r, k) > 1 \) we have \( G(r, \chi) \neq 0 \).

Suppose, then, that \( \chi \) is not primitive modulo \( k \). This implies \( k > 1 \).

Then \( \chi \) has a conductor \( d < k \). If \( d = 1 \) then \( \chi = \chi_1 \) and we have

\[
G(r, \chi_1) = \sum_{h \mod k} \chi_1(h)e^{2\pi irh/k} = \sum_{h \mod k; (h, k) = 1} e^{2\pi irh/k}.
\]

When \( r = k \) we have \( G(k, \chi_1) = \phi(k) \neq 0 \). This proves the lemma for the case in which the conductor \( d = 1 \).

Now suppose \( d > 1 \) and let \( r = k/d \). We have \( (r, k) > 1 \) and we shall prove that \( G(r, \chi) \neq 0 \) for this \( r \). By Lemma 5 there exists a character \( \psi \) modulo \( d \) such that \( \chi(n) = \psi(n)\chi_1(n) \) for all \( n \). Hence we can write

\[
G(r, \chi) = \sum_{h \mod k} \psi(h)\chi_1(h)e^{2\pi irh/k} = \sum_{h \mod k; (h, k) = 1} \psi(h)e^{2\pi irh/k} = \frac{\phi(k)}{\phi(d)} \sum_{h \mod d; (h, d) = 1} \psi(h)e^{2\pi irh/d},
\]

where in the last step we used Lemma 6. Therefore we have

\[
G(r, \chi) = \frac{\phi(k)}{\phi(d)} G(1, \psi).
\]

But \( |G(1, \psi)|^2 = d \) by Lemma 4 (since \( \psi \) is primitive modulo \( d \)) and hence \( G(r, \chi) \neq 0 \). This completes the proof of Lemma 7. As already mentioned, Lemmas 3 and 7 together prove Theorem 1.

**References**


**California Institute of Technology**