EULER'S ϕ-FUNCTION AND SEPARABLE GAUSS SUMS

TOM M. APOSTOL

1. **Introduction.** Let k denote a fixed positive integer. A completely multiplicative arithmetical function χ is called a *character* modulo k if χ 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 χ_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 χ if we have

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

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

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

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

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

$$G(r, \chi) = \bar{\chi}(r) G(1, \chi). \tag{3}$$

It is well known that the Gauss sum $G(r, \chi)$ is separable if χ 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 χ is primitive. Therefore, we have the following alternate description of primitive characters.

THEOREM 1. *A character χ 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 ϕ-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 χ 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 $\chi(h) =\bar{\chi}(r)\chi(r)\chi(h)=\bar{\chi}(r)\chi(rh)$. Hence we can write

$$G(r, \chi) = \sum_{h \bmod k} \chi(h)e^{2\pi irh/k} = \bar{\chi}(r) \sum_{h \bmod k} \chi(rh)e^{2\pi irh/k}$$
$$= \bar{\chi}(r) \sum_{m \bmod k} \chi(m)e^{2\pi im/k} = \bar{\chi}(r)G(1, \chi).$$

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 $\bar{\chi}(r)=0$ so equation (3) holds if and only if $G(r, \chi)=0$.

LEMMA 3. *If χ 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 χ 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 χ be any character modulo k and let d be the conductor of χ. Then there exists a primitive character ψ modulo d such that*

$$\chi(n) = \psi(n)\chi_1(n), \tag{4}$$

where χ_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 ψ is a character modulo d. To prove that ψ is a *primitive* character modulo d, let q be any induced modulus for ψ. Then we have

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

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 χ. Hence $q \geqq d$ since d is the conductor of χ. Therefore the conductor of ψ is equal to d so ψ 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: $S_k \rightarrow S_d$ as follows:

$$\text{If } n \in S_k, \qquad \text{then } f(n) = r, \quad \text{where} \quad n \equiv r \pmod{d}.$$

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

$$x \equiv r \pmod{d}, \qquad x \equiv 1 \pmod{k'},$$

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 $n \equiv 1 \pmod{k'}$ and that $(n, d) = 1$ because $n \equiv r \pmod{d}$. 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 χ modulo k has separable Gauss sums $G(r, \chi)$ for every r, then χ is primitive modulo k.*

PROOF. Because of Lemmas 1 and 2, it suffices to prove that if χ is not primitive then for some r satisfying $(r, k)>1$ we have $G(r, \chi)\neq 0$. Suppose, then, that χ is not primitive modulo k. This implies $k>1$. Then χ has a conductor $d<k$. If $d=1$ then $\chi=\chi_1$ and we have

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

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 ψ modulo d such that $\chi(n)=\psi(n)\chi_1(n)$ for all n. Hence we can write

$$G(r, \chi) = \sum_{h \bmod k} \psi(h)\chi_1(h)e^{2\pi irh/k} = \sum_{h \bmod k;\ (h,k)=1} \psi(h)e^{2\pi irh/k}$$

$$= \sum_{h \bmod k;\ (h,k)=1} \psi(h)e^{2\pi ih/d} = \frac{\phi(k)}{\phi(d)} \sum_{h \bmod d;\ (h,d)=1} \psi(h)e^{2\pi ih/d},$$

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 ψ 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

1. Tom M. Apostol, *Resultants of cyclotomic polynomials*, Proc. Amer. Math. Soc. 24 (1970), 457–462.

2. Raymond Ayoub, *An introduction to the analytic theory of numbers*, Mathematical Surveys, no. 10, Amer. Math. Soc., Providence, R. I., 1963. MR 28 #3954.

3. Trygve Nagell, *Zahlentheoretische Notizen*, Skr. Norske Vid. Akad. Oslo I 13 (1923), 23–25.

4. Karl Prachar, *Primzahlverteilung*, Springer-Verlag, Berlin, 1957. MR 19, 393.

5. R. Vaidyanathaswamy, *A remarkable property of the integers mod n and its bearing on group theory*, Proc. Indian Acad. Sci. Sec. A 5 (1937), 63–75.

CALIFORNIA INSTITUTE OF TECHNOLOGY