GENERALIZATIONS OF THE EULER φ-FUNCTION

By Harlan Stevens

1. Introduction. Generalizations of the Euler φ-function have a history rich in discovery and, perhaps not surprisingly, rediscovery. The totients of H. L. Alder [1] and D. N. Lehmer [7], for example, are covered by Nagell's totient [10], which is itself a special case of Lucas' [8; 402] extension of Schemmel's function [11]. An examination of Dickson's History [4, Chapter V] shows that Jordan's totient $J_k(n)$ has also appeared in many guises. (For definitions of these functions see the examples in §2.) The purpose of this paper is to discuss a very general totient function which subsumes and extends those above along with many of their identities. Although other authors, notably Eckford Cohen and P. J. McCarthy, have considered similar questions, their viewpoint is substantially different (e.g. [3], [9]).

Our main results are set forth in Definition 1 and Formulas (1), (4), (5), (6), and (10).

2. The $\varphi(F, n)$-function. We begin with the following arithmetic function.

Definition 1. *Let* $F = \{f_1(x), \cdots, f_k(x)\}$ *be a set of polynomials with integral coefficients, and let* $A = \{(a_1, \cdots, a_k), \cdots\}$ *be the set of all ordered* k*-tuples of integers such that* $0 \leq a_i < n$. *Then* $\varphi(F, n)$ *is the number of elements in* A *such that the* G.C.D. $(f_1(a_1), \cdots, f_k(a_k), n) = 1$.

From here on we will always write explicitly "the k-tuple $(a_1, \cdots, a_k)$" to distinguish it from the greatest common divisor. Two k-tuples $(a_1, \cdots, a_k)$ and $(b_1, \cdots, b_k)$ are said to be congruent (mod n) if $a_i \equiv b_i \pmod{n}$ for each i, and a k-complete residue system is any set of n^k incongruent k-tuples. Thus to compute $\varphi(F, n)$ we may consider $(f_1(a_1), \cdots, f_k(a_k), n)$ evaluated over any k-complete residue system.

To find a formula for $\varphi(F, n)$ we set $n = rs$, where $(r, s) = 1$, and show that

$$\varphi(F, r)\varphi(F, s) = \varphi(F, n);$$

that is, that $\varphi(F, n)$ is multiplicative. We do this by first determining the subset of A such that $(f_1(a_1), \cdots, f(a_k), r) = 1$, and then the subset of this subset such that $(f_1(a_1), \cdots, f_k(a_k), s) = 1$. Clearly, the order of this set is $\varphi(F, rs)$.

Now every integer $a_\mu (0 \leq a_\mu < rs)$ can be expressed uniquely as

$$a_\mu = i_\mu r + j_\mu \qquad (0 \leq i_\mu < s, \quad 0 \leq j_\mu < r).$$

Received April 18, 1969.