PRIMITIVE ROOTS THE CYCLOTOMIC WAY

Joseph B. Dence

1. Introduction. Every prime possesses a primitive root. So stated (in an equivalent way) J. H. Lambert in 1769; Legendre gave the first correct proof in 1785. Gauss, in 1801, published two proofs in his *Disquisitiones Arithmeticae* [3a]. This important theorem is standard material in any first course in number theory. A survey of 21 number theory texts, both old and recent, shows the following distribution of proofs:

(1) 13 texts prove the theorem with the aid of the following lemma on the Euler ϕ-function [1a–l,5a]:

$$\sum_{d|n} \phi(d) = n;$$

(2) 2 texts use the Möbius Inversion Formula, together with the lemma,

$$\sum_{d|n} \mu(d)(n/d) = \phi(n),$$

also drawn from material on multiplicative functions [1f,m];

(3) 4 texts use only elementary facts on the orders of integers, and possibly also Lagrange's Theorem on roots in a field [1n–q];

(4) 2 texts use only Lagrange's Theorem and the concept of the least (or minimal) universal exponent (first introduced by R. D. Carmichael) [1r,s];

(5) 1 text employs an algebraic proof that considers the generation of various subgroups of $\mathbb{Z}_p^x$ [1f];

(6) 1 text uses Lagrange's Theorem, together with a key result on orders of elements in finite Abelian groups [1t].

All of the above methods of proof have features of interest, and there are pros and cons of each. Gauss' own proofs belonged to methods (1) and (3).