QUESTION

(i) Define the Möbius function, $\mu(n)$.

(ii) Let G denote the cyclic group of order n. For each positive integer, d, dividing n set

$$f(d) = |\{g \in G | \text{order}(g) = d\}|,$$

the number of elements of order d in G. Use the Möbius Inversion Formula to show that

$$f(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) d,$$

where the sum is over all positive divisors of n.

(iii) What is the relation between (ii) and Euler's function, $\phi(n)$?

ANSWER

(i) By definition

$$\mu n = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n > 1 \text{ and } p^2|n \text{ for some prime } p, \\ (-1)^t & \text{if } n \text{ is the product of } t \text{ distinct primes.} \end{cases}$$

(ii) Every element of G has precisely one order, D, which divides n. Since G is cyclic every possible d occurs as the order of some element. Hence we have

$$n = |G| = \sum_{d|n} f(d) = F(n).$$

By the Möbius Inversion Formula

$$f(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) F(d) = \sum_{d|n} \mu\left(\frac{n}{d}\right) d.$$

(iii) Let $g \in G$ denote a generator. The element of G of order n are precisely the g^j with $\gcd(j, n) = 1$. Also distinct such j's give rise to distinct g^j's so that $f(n) = \phi(n)$. The formula

$$\phi(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) d$$