QUESTION

(i) Give, without proof, a formula for Euler's function, $\phi(n)$, in terms of the prime power factorisation of n.

(ii) Let m and n be positive integers such that $\mathrm{HCF}(m, n) = d$. Show that

$$\phi(d)\phi(mn) = \phi(m)\phi(n)d.$$

(iii) Hence show that

$$\phi(mn) \leq \phi(m)\phi(n)$$

with equality if and only if $\mathrm{HCF}(m, n) = 1$.

(iv) Define what is meant by the multiplicative order of a congruence class, $[x] \in U_m$, where U_m denotes the group of units mod (m).

(v) Suppose that there exists an integer, x, such that $\mathrm{HCF}(x, m) = 1$ and the order of $[x]$ in U_m is equal to $m - 1$. Using Euler's Theorem, or otherwise, show that m is prime.

ANSWER

(i) If $n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$ where the p_i's are distinct primes and the $a_i \geq 1$ are integers then

$$\phi(n) = p_1^{a_1-1} p_2^{a_2-1} \dots p_k^{a_k-1} \prod_{j=1}^{k} (p_j - 1)$$

(ii) To prove this one we change notation a little. Let $p_1, \dots, p_k$ denote the set of distinct primes which appear to a strictly positive exponent in the prime power factorisation of at least one of m or n. Hence we may write

$$n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}, m = p_1^{b_1} p_2^{b_2} \dots p_k^{b_k}$$

with each $a_i \geq 0$ and $b_i \geq 0$ but $a_i + b_i > 0$ for each i. In this case

$$d = \prod_{i=1}^{k} p_i^{min(a_i, b_i)}$$

Hence the left hand side is equal to

$$\left(\prod_{i=1}^{k} p_i^{min(a_i,b_i)-1}(p_i-1)\right)\left(\prod_{j=1}^{k} p_j^{a_j+b_j-1}(p_j-1)\right)$$

where in the first factor only i's with $min(a_i,b_i) \geq 1$ appear.

On the right hand side we have

$$\left(\prod_{i=1}^{k} p_i^{min(a_i,b_i)}\right)\left(\prod_{u=1}^{k} p_u^{a_u-1}(p_u-1)\right)\left(\prod_{j=1}^{k} p_j^{b_j-1}(p_j-1)\right)$$

where in second factor only u's with $a_u \geq 1$ appear and in the third factor only j's with $b_j \geq 1$ appear.

Now look at the occurrence of p_i and (p_i-1)'s on both sides. On the left we find

$$\begin{array}{ll} p_i^{min(a_i,b_i)-1}(p_i-1)p_i^{a_i+b_i-1}(p_i-1) & \text{if } \min(a_i,b_i) \geq 1, \\ p_i^{a_i+b_i-1}(p_i-1) & \text{if } \min(a_i,b_i) = 0 \end{array}$$

On the right we find

$$\begin{array}{ll} p_i^{min(a_i,b_i)}p_i^{a_i-1}(p_i-1)p_i^{b_i-1}(p_i-1) & \text{if } a_i \geq 1 \text{ and } b_i \geq 1, \\ p_i^{min(a_i,b_i)}p_i^{b_i-1}(p_i-1) & \text{if } a_1 = 0 \text{ and } b_1 \geq 1, \\ p_i^{min(a_i,b_i)}p_i^{a_i-1}(p_i-1) & \text{if } a_i \geq 1 \text{ and } b_i = 0. \end{array}$$

These expressions are equal.

(iii) If $d > 1$ then $\phi(d) < d$ by the formula of (i) while $\phi(1) = 1$.

(iv) The order of a congruence class $[x] \in U_m$ is the least positive integer, k, such that $x^k \equiv 1 \bmod (m)$.

(v) By Euler's Theorem we know that $x^{\phi(m)} \equiv 1 \bmod (m)$ and therefore that the order of x divides $\phi(m)$. Hence m is such that $(m-1)|\phi(m)$. Since $\phi(m) < m$ for $m > 1$ we must have $\phi(m) = m - 1$ which implies that m is prime, by the formula of (i).