QUESTION

An integer $n \geq 1$ is called a *Carmichael number* if n is not a prime and $a^{n-1} \equiv 1$ (modulo n) for all integers a such that $\gcd(a, n) = 1$. Throughout this question let n denote a Carmichael number..

(i) Show that n cannot be a power of 2.

(ii) Let p be an odd prime such that p^α divides n with $\alpha \geq 1$. Show that $\alpha = 1$ and $p-1$ divides $n-1$. (Hint: You may need to use the Chinese Remainder Theorem to make a good choice of α. Also you may assume that the group of units modulo p^α, usually denoted by U_{p^α}, is cyclic of order $\phi(p^\alpha)$.)

(iii) Use part (ii) to show that n is odd.

(iv) Show that $n = p_1 p_2 \dots p_r$ where $p_1, \dots, p_r$ are distinct odd primes and $r \geq 3$.

ANSWER

(i) Suppose that $n = 2^\alpha$, Then $\alpha = 1$ corresponds to $n = 2$, which is prime, while for $\alpha \geq 2$ we may take $a = -1$ to obtain

$$a^{2^\alpha - 1} = (-1)^{2^\alpha - 1} = -1$$

which is not congruent to 1 modulo 4 much less modulo a^α.

(ii) Write $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ with each $\alpha_i \geq 1$ and $p_1, \dots p_r$ distinct primes. Suppose that the odd prime p is p_1 so that $\alpha = \alpha_1$. By the Chinese Remainder Theorem we may choose an integer, a, such that

$$a = \begin{cases} x & \text{(modulo } p_1^{\alpha_1}\text{)}, \\ 1 & \text{(modulo } p_i\text{) for } i = 2, \dots r \end{cases}$$

where the multiplicative order of x modulo $p_1^{\alpha_1}$ is $\phi(p_1^{\alpha_1}) = p_1^{\alpha_1 - 1}(p_1 - 1)$. Such a choice of a satisfies $\gcd(a, n) = 1$. Then $a^{n-1} \equiv 1$ (modulo n) implies that $x^{n-1} \equiv a^{n-1} \equiv 1$ (modulo $p_1^{\alpha_1}$). Therefore $p_1^{\alpha_1 - 1}(p_1 - 1)$ divides $n - 1 = p_1^{\alpha_1} \dots p_r^{\alpha_r} - 1$. If $\alpha_1 \geq 2$ then p_1 would divide 1 so we must have $\alpha_1 = 1$. In this case the condition that $\phi(p_1^{\alpha_1})$ divides $n - 1$ becomes simply $p_1 == 1$ divides $n - 1$, as required.

(iii) By part (i), $r \geq 2$ in part (ii) and so one of the primes dividing n is odd. By part (ii). $n - 1$ is even because it is divisible by $p - 1$ for some odd prime. Hence n is odd.

(iv) By parts (ii) and (ii), n is a product of distinct odd primes. It remains to show that $n = p_1 p_2$ is not a carmichael number when p_1 and p_2 are distinct primes. However the equation

$$n - 1 = p_1 p_2 - 1 = (p_1 - 1)(p_2 + (p_2 - 1)$$

together with part (ii) would imply that $(p_2 - 1)$ divides $(p_1 - 1)$ and vice versa. This would imply the contradiction that $p_1 = p_2$.