

1 Suppose that m does not have a primitive root. Show that
 PEN B6

$$a^{\frac{\varphi(m)}{2}} \equiv 1 \pmod{m}$$

for every a relatively prime to m .

First, we use the well known fact that m has primitive roots if and only if m has the form $2, 4, p^k$ or $2p^k$ where p is an odd prime number and k is a positive integer. We thus have to prove the statement for all other numbers.

First Solution. First, notice that if m has no primitive roots and is not a power of 2, then we can write m as $m = m_1 m_2$ where m_1 and m_2 are relatively prime positive integers satisfying $2 \mid \varphi(m_1)$ and $2 \mid \varphi(m_2)$. Since $a^{\varphi(m_1)} \equiv 1 \pmod{m_1}$ for every integer a coprime to m_1 and $a^{\varphi(m_2)} \equiv 1 \pmod{m_2}$ for every integer a coprime to m_2 , we have

$$a^{\varphi(m_1) \frac{\varphi(m_2)}{2}} \equiv 1 \pmod{m_1}$$

and

$$a^{\varphi(m_2) \frac{\varphi(m_1)}{2}} \equiv 1 \pmod{m_2}$$

for every integer a coprime to $m_1 m_2 = m$. Thus, by the Chinese Remainder Theorem, it follows that

$$a^{\frac{\varphi(m_1)\varphi(m_2)}{2}} = a^{\frac{\varphi(m)}{2}} \equiv 1 \pmod{m_1 m_2 = m}$$

which proves the proposition for all desired m that are not a power of 2.

Suppose now that $m = 2^k$ is a power of 2 and has no primitive roots. Notice that $k \geq 3$. The proof of the claim goes by induction on k .

For $k = 3$, we can simply check that $a^{\frac{\varphi(8)}{2}} = a^2 \equiv 1 \pmod{8}$ for all odd a (we have $1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \pmod{8}$). Suppose now that $a^{\frac{\varphi(2^k)}{2}} = a^{2^{k-2}} \equiv 1 \pmod{2^k}$ for some positive integer $k \geq 3$ and every odd integer a . Then for every such a , we either have

$$a^{2^{k-2}} \equiv 1 \pmod{2^{k+1}}$$

or

$$a^{2^{k-2}} \equiv 1 + 2^k \pmod{2^{k+1}}.$$

In the first case, we trivially have

$$a^{2^{k-1}} \equiv 1 \pmod{2^{k+1}}$$

and in the second case, we have

$$a^{2^{k-1}} \equiv (1 + 2^k)^2 \equiv 1 + 2^{k+1} + 2^{2k} \equiv 1 + 2^{2k} \pmod{2^{k+1}}$$

and since $k \geq 3$, we have $2k \geq k + 1$ and thus

$$a^{2^{k-1}} \equiv a^{\frac{\varphi(2^{k+1})}{2}} \equiv 1 \pmod{2^{k+1}}$$

which proves the induction step. □

Second Solution. From a more advanced and more general point of view, we can analyze the smallest positive integer t , so that $a^t \equiv 1 \pmod{m}$ for every integer a coprime to m , where m is a given positive integer.

Definition 1. Let m be a positive integer. Then $\lambda(m)$ denotes the least positive integer t so that

$$a^t \equiv 1 \pmod{m}$$

holds for all integers a coprime to m . λ is called the Carmichael Function.

We start with an easy lemma:

Lemma 1. Let m and t be positive integers. Then

$$a^t \equiv 1 \pmod{m}$$

holds for every integer a coprime to m if and only if $\lambda(m) \mid t$. In particular, $\lambda(m) \mid \varphi(m)$.

Proof. The claim is trivial if $\lambda(m) \mid t$. On the other hand, if

$$a^t \equiv 1 \pmod{m}$$

holds for every integer a coprime to m , then by the integer division algorithm, there exist integers q and r so that $t = q\lambda(m) + r$ and $0 \leq r < \lambda(m)$. Thus, for every integer a coprime to m , we have

$$1 \equiv a^t \equiv a^{q\lambda(m)+r} \equiv a^{q\lambda(m)} \cdot a^r \equiv a^r \pmod{m}.$$

But $r < \lambda(m)$ and since we have defined $\lambda(m)$ as the smallest positive integer with this property, this implies $r = 0$ and thus $\lambda(m) \mid t$. \square

In order to solve the problem, we can derive a (well known) formula for $\lambda(m)$:

Proposition 1. Let $m \geq 2$ be a positive integer. Then

$$\lambda(m) = \varphi(m) \quad \text{if } m = 2, 4, p^k \text{ where } p \text{ is an odd prime and } k \in \mathbb{Z}^+ \quad (1)$$

$$\lambda(m) = 2^{k-2} \quad \text{if } m = 2^k \text{ where } k \geq 3 \text{ is an integer} \quad (2)$$

$$\lambda(m) = \text{lcm}(\lambda(p_1^{k_1}), \dots, \lambda(p_r^{k_r})) \quad \text{if } m = p_1^{k_1} \dots p_r^{k_r} \text{ is the prime factorization of } m. \quad (3)$$

Proof. (1) directly follows from the existence of primitive roots modulo $m = 2, 4, p^k$.

For (2), we can, as in the first proof of this problem, first show that if $k \geq 3$ is an integer, then

$$a^{2^{k-2}} \equiv 1 \pmod{2^k}$$

for every odd integer a (which implies that $\lambda(2^k) \leq 2^{k-2}$). Next, we can show by induction on k that there exists an odd integer a which satisfies $\text{ord}_{2^k}(a) = 2^{k-2}$ for every integer $k \geq 3$ (which implies the minimality of 2^{k-2}).

This is clear if $k = 3$ or $k = 4$, simply take $a = 3$ for example and observe that $\text{ord}_8(3) = 2$ and $\text{ord}_{16}(3) = 4$.

Suppose now that for some integer $k \geq 4$ and some odd integer a , we have

$$\text{ord}_{2^{k-1}}(a) = 2^{k-3} \quad \text{and} \quad \text{ord}_{2^k}(a) = 2^{k-2}.$$

This however implies that

$$a^{2^{k-3}} \equiv 1 \pmod{2^{k-1}} \quad \text{but} \quad a^{2^{k-3}} \not\equiv 1 \pmod{2^k},$$

so

$$a^{2^{k-3}} \equiv 1 + 2^{k-1} \pmod{2^k}$$

and thus, we either have

$$a^{2^{k-3}} \equiv 1 + 2^{k-1} \pmod{2^{k+1}}$$

or

$$a^{2^{k-3}} \equiv 1 + 2^{k-1} + 2^k \pmod{2^{k+1}}.$$

In the first case, we have

$$a^{2^{k-2}} \equiv (1 + 2^{k-1})^2 \equiv 1 + 2^k + 2^{2k-2} \equiv 1 + 2^k \not\equiv 1 \pmod{2^{k+1}}$$

and in the second case, we have

$$a^{2^{k-2}} \equiv (1 + 2^{k-1} + 2^k)^2 \equiv 1 + 2^{2k-2} + 2^{2k} + 2^k + 2^{k+1} + 2^{2k} \equiv 1 + 2^k \not\equiv 1 \pmod{2^{k+1}}.$$

So in both cases, we have $a^{2^{k-2}} \not\equiv 1 \pmod{2^{k+1}}$ and since $\text{ord}_{2^{k+1}}(a) \mid \varphi(2^{k+1}) = 2^k$, we have $\text{ord}_{2^{k+1}}(a) \geq 2^{k-1}$. But we already know that $\lambda(2^{k+1}) \leq 2^{k-1}$ and since $\text{ord}_{2^{k+1}}(a) \leq \lambda(2^{k+1})$, this implies $\text{ord}_{2^{k+1}}(a) = 2^{k-1}$ and thus $\lambda(2^{k+1}) = 2^{k-1}$. This proves the equation (2)

For (3), assume that $m = m_1 m_2$ where $m_1, m_2 > 1$ are coprime positive integers. Then by the chinese remainder theorem,

$$a^t \equiv 1 \pmod{m} \tag{4}$$

holds for every integer a coprime to m if and only if

$$a^t \equiv 1 \pmod{m_1}$$

holds for every integer a coprime to m_1 and

$$a^t \equiv 1 \pmod{m_2}$$

holds for every integer a coprime to m_2 .

However, by Lemma 1, the latter holds if and only if

$$\lambda(m_1) \mid t \quad \text{and} \quad \lambda(m_2) \mid t \tag{5}$$

and since we have defined $\lambda(m)$ as the smallest positive integer t which satisfies (4) and thus the smallest positive integer satisfying (5), we obtain

$$\lambda(m) = \text{lcm}(\lambda(m_1), \lambda(m_2)),$$

which proves (3) and thus Proposition 1. □

From Proposition 1, we immediately infer that

Corollary 1. *Let $m \geq 2$ be a positive integer. Then $\lambda(m) = \varphi(m)$ if and only if $m = 2, 4, p^k, 2p^k$ where p is an odd prime number and k is a positive integer. For all other m we have $\lambda(m) < \varphi(m)$ and since $\lambda(m) \mid \varphi(m)$ by Lemma 1, we have $\lambda(m) \leq \varphi(m)/2$.*

It thus remains to be proven that if m has no primitive roots, then $\lambda(m) \mid \varphi(m)/2$. This is clear if $m \geq 8$ is a power of two. Otherwise, by (3) of Proposition 1, we have at least two coprime divisors m_1 and m_2 with $\varphi(m_1), \varphi(m_2)$ being even, which implies that at least one factor 2 drops out of $\varphi(m)$ if compared to $\lambda(m)$. This solves the problem. \square