Euler's $\phi$ Function and Euler's Theorem

Q: Let $a \in \mathbb{Z}$ be coprime to the prime $p$. What is a power of $a$ is guaranteed to be congruent to 1 modulo $p$?

A: $p-1$ by FLT

Q2: Let $a, m \in \mathbb{Z}$ with $m > 1$ and $(a, m) = 1$. What is power of $a$ is guaranteed to be congruent to 1 modulo $m$?

A: Given by Euler's Thm.

We need a preliminary definition:

Def: Let $m \in \mathbb{Z}_{>0}$. The Euler $\phi$-function is given by

$$\phi(m) = \# \{ x \in \mathbb{Z} : 1 \leq x < m, 1 \text{ and } (x, m) = 1 \}$$

that is, the number of positive integers up to $m$ that are coprime to $m$.

Examples:

$\phi(1) = 1$
$\phi(2) = 1$
$\phi(3) = 2$ because $1, 2$ are coprime to $3$
$\phi(6) = 2$ because $1, 2, 3, 4, 5$ only $1, 5$ are coprime to $6$

$\phi(p) = p-1$ if $p$ is prime
Theorem (Euler): Let \( a, m \in \mathbb{Z} \) with \( m > 0 \) and such that \( (a, m) = 1 \).
Then \( a^{\phi(m)} \equiv 1 \pmod{m} \)

Corollary (FLT): Let \( m = p \) be prime.
Then \( \phi(p) = p-1 \) and \( a^{p-1} \equiv 1 \pmod{p} \)

Proof of Euler's Theorem:

Let \( a_1, a_2, \ldots, a_{\phi(m)} \) be the distinct positive integers \( \leq m \) such that \( (a_i, m) = 1 \) (by definition of \( \phi(m) \)).

We claim that \( a^1 a_1, a^2 a_2, \ldots, a^m a_{\phi(m)} \) are \( \phi(m) \) integers s.t. \( (a - a_i, m) = 1 \) and no two of them are congruent modulo \( m \).

Therefore

\[
(a^1 a_1)(a^2 a_2) \cdots (a^m a_{\phi(m)}) \equiv a_1 a_2 \cdots a_{\phi(m)} \pmod{m}.
\]

\[
\implies a^{\phi(m)} a_1 a_2 \cdots a_{\phi(m)} \equiv a_1 a_2 \cdots a_{\phi(m)} \pmod{m}.
\]

Since \( (a_1 a_2 \cdots a_{\phi(m)}, m) = 1 \) the number \( a_1 a_2 \cdots a_{\phi(m)} \) is invertible mod \( m \) hence

\[
a^{\phi(m)} \equiv 1 \pmod{m}.
\]
We now prove the claim.

1. Suppose \((a \cdot a_i, m) > 1\) for some \(i\).
   Then \(\exists p \neq 1\) such that \(p\mid a_i\) and \(p\mid m\).

\[ \Rightarrow (p \mid a \text{ AND } p \mid m) \lor (p \mid a_i \text{ AND } p \mid m) \]

\[ \Rightarrow (a, m) > 1 \text{ OR } (a_i, m) > 1, \text{ CONTRADITION!} \]

2. Suppose \(a \cdot a_i \equiv a \cdot a_j \pmod{m}\). Since \((a, m) = 1\), the inverse \(a^{-1}\) exists and we have

\[ a^{-1}(a \cdot a_i) \equiv a^{-1}(a \cdot a_j) \pmod{m} \]

\[ \Rightarrow a_i \equiv a_j \pmod{m} \text{ where } 0 \leq a_i, a_j \leq m-1 \]

\[ \Rightarrow a_i = a_j \]

**Def:** A set of integers with \(\phi(m)\) elements which are coprime to \(m\) and no two of them are congruent modulo \(m\) is a **Reduced Residue System modulo** \(m\).

**Corollary** (of the claim): Let \(a \in \mathbb{Z}_m\), \((a, m) = 1\).

If \(\{a_1, a_2, \ldots, a_{\phi(m)}\}\) is a reduced residue system modulo \(m\), then \(\{a \cdot a_1, a \cdot a_2, \ldots, a \cdot a_{\phi(m)}\}\) also is
Theorem (formula for $\phi$): Let $m = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$. Then \[ \phi(m) = m \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right) \]

Example: $\phi(100) = \phi(2^2 \cdot 5^2) = 100 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{5}\right) = 40$

Ex: Compute the last 2 digits of $3^{50}$.

WANT: $3^{50} \equiv \text{(mod 100)}$ because 40 $\phi(100) \leq \text{theorem}$

\[ 3^{50} \equiv 3 \cdot 3 \equiv 4 \cdot 3 \equiv 2 \cdot 3 \equiv 3 \equiv 7 \equiv 9 \equiv 49 \text{ (mod 100)} \]

Example: Solve the equation $\phi(m) = 8$.

let $m = p_1^{a_1} \cdots p_k^{a_k}$. Then $\phi(m) = \frac{k}{\prod_{j=1}^{k} p_j^{a_j-1}} (p_j - 1)$.

$\phi(m) = 8 \Rightarrow p_j \leq 7$ otherwise $\phi(m) > p_j - 1 > 8$

$P_j \neq 7$ otherwise $p_j - 1 = 6 | \phi(m) = 8$ impossible. Thus $m = 2^a3^b5^c$

Moreover $b = 0$ or $b = 1$ otherwise $3 | 8$; similarly $c = 0$ or $c = 1$.

Now we have 4 cases to check:

1. $a = c = 0 \Rightarrow m = 2^a \Rightarrow \phi(m) = 2^{a-1} = 2 \Rightarrow a = 4 \Rightarrow m = 16$

2. $b = 0, c = 1 \Rightarrow m = 2^a5^b \Rightarrow \phi(m) = 2^{a-1} \cdot 4 = 8 \Rightarrow a = 2 \Rightarrow m = 20$

3. $b = 1, c = 0 \Rightarrow m = 2^a3^b \Rightarrow \phi(m) = 2^a \cdot 2 = 8 \Rightarrow a = 3 \Rightarrow m = 24$

4. $b = c = 1 \Rightarrow m = 2^a3^b5^c \Rightarrow \phi(m) = 2^a \cdot 2 \cdot 4 = 8 \Rightarrow a = 1 \Rightarrow m = 30$

If $a = 0$ then $m = 15$ and $\phi(m) = 8$ also works.
**Arithmetic Functions**

Def: A function whose domain is \( \mathbb{Z}_{>0} \)

is called an **Arithmetic Function**

Examples:

1. \( f(m) = 1 \quad \forall m \)
2. \( f(m) = m \quad \forall m \)
3. \( \varphi(m) \) "the Euler \( \varphi \)-function"
4. \( \tau(m) = \) "number of positive divisors of \( m \)"
5. \( \sigma(m) = \) "sum of positive divisors of \( m \)"

Ex: Take \( m = 6 \). Its positive divisors are \( \{1, 2, 3, 6\} \).

Thus \( \tau(6) = 4 \) and \( \sigma(6) = 1 + 2 + 3 + 6 = 12 \)

Def: An arithmetic function \( f \) is called

multiplicative if \( f(m_1 \cdot m_2) = f(m_1) \cdot f(m_2) \)

whenever \( (m_1, m_2) = 1 \).

\( f \) is called completely multiplicative

if \( f(m_1 \cdot m_2) = f(m_1)f(m_2) \quad \forall m_1, m_2 \)
Theorem: The function $\phi(m)$ is multiplicative.

Proof: Let $m_1, m_2 > 0$ be coprime.

WANT: $\phi(m_1 \cdot m_2) = \phi(m_1) \cdot \phi(m_2)$

We write the positive integers up to $m_1 \cdot m_2$ in the form:

1. $m_1 + 1 \quad 2m_1 + 1 \quad \ldots \quad (m_2 - 1)m_1 + 1$
2. $m_1 + 2 \quad 2m_1 + 2 \quad \ldots \quad (m_2 - 1)m_2 + 2$
3. $m_1 + 3 \quad 2m_1 + 3 \quad \ldots \quad (m_2 - 1)m_2 + 3$
   \vdots
4. $m_1 + n \quad 2m_1 + n \quad \ldots \quad (m_2 - 1)m_1 + n$
   \vdots
5. $m_1 \quad 2m_1 \quad 3m_1 \quad \ldots \quad m_1 \cdot m_2$

- Suppose $1 \leq n \leq m_1$ and $(n, m_1) = d > 1$

Then all the numbers in the $n$-th row are divisible by $d$.

Thus they are not coprime to $m_1 \cdot m_2$.

- Hence there are $\phi(m_1)$ rows that may contain numbers which are coprime to $m_1 \cdot m_2$.

Suppose $(n, m_1) = 1$. It follows that the elements in the $n$-th row are coprime to $m_1$.

The $n$-th row has $m_2 - 1$ elements which are not congruent modulo $m_2$ because

$k \cdot m_1 + n \equiv k' \cdot m_1 + n \pmod{m_2}$

$\Rightarrow k \equiv k' \pmod{m_2} \Rightarrow k = k'$
Thus exactly \( \phi(m_2) \) of them are coprime to \( m_2 \).

Since they are also coprime to \( m_1 \), then they are coprime to \( m_1 m_2 \).

Here is a method to produce multiplicative functions:

Then: let \( f \) be an arithmetic function. Define the arithmetic function \( F \) by

\[
F(n) = \sum_{d|n} f(d) \quad \forall n \in \mathbb{Z}_{>0}
\]

If \( f \) is multiplicative then \( F \) is multiplicative.
Theorems: \( \sigma(m) \) and \( \tau(m) \) are multiplicative functions.

Proof: We can write \( \tau \) and \( \sigma \) as

\[
\tau(m) = \sum_{d \mid m} 1, \quad \sigma(m) = \sum_{d \mid m} d
\]

Since \( f(m) = 1 \) and \( f(m) = m \) are multiplicative functions, the result follows from the previous theorem. \( \square \)
Lecture 17

ARITHMETIC FUNCTIONS CONTINUED

Theorem: Let $f$ be an arithmetic function. Define the function $F$ by

$$F(m) = \sum_{d|m, d>0} f(d) \quad \forall m \in \mathbb{Z}_{>0}$$

If $f$ is multiplicative then $F$ is also multiplicative.

Corollary: $T(m)$ and $\sigma(m)$ are multiplicative functions.

Proof of Theorem:

\begin{align*}
\text{WANT: } F(m_1 \cdot m_2) &= F(m_1) \cdot F(m_2) \\
\text{when } (m_1, m_2) &= 1
\end{align*}

We have

$$F(m_1 \cdot m_2) = \sum_{d|m_1 \cdot m_2, d>0} f(d)$$
Since \((m_1, m_2) = 1\) each divisor \(d\) of \(m_1 m_2\) can be written as \(d = d_1 \cdot d_2\), where \((d_1, d_2) = 1\), \(d_1 \mid m_1\), \(d_2 \mid m_2\).

Also, each such product \(d_1 \cdot d_2\) is a divisor of \(m_1 m_2\).

Thus

\[
F(m_1 m_2) = \sum_{d \mid m_1 m_2, d > 0} f(d) = \sum_{d_1 \mid m_1, d_2 \mid m_2, d_1 > 0, d_2 > 0} f(d_1 d_2)
\]

\[
= \sum_{d_1 \mid m_1, d_2 \mid m_2, d_1 > 0, d_2 > 0} f(d_1) \cdot f(d_2) =
\]

\[
= \left(\sum_{d_1 \mid m_1, d_1 > 0} f(d_1)\right) \left(\sum_{d_2 \mid m_2, d_2 > 0} f(d_2)\right)
\]

\[
= F(m_1) \cdot F(m_2) \]
Formulas for $\phi, \sigma, \tau$

Let $m = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$ with $p_i$ distinct.

Let $f$ be $\phi, \sigma, \tau$. Then

$$f(m) = f(p_1^{a_1}) \cdot f(p_2^{a_2}) \cdots f(p_n^{a_n})$$

Thus to find a formula for $f$ it is enough to find it for $f(p_i^{a_i})$.

**Lemma:** $\phi(p^a) = p^a - p^{a-1} = p^a(1 - 1/p)$

**Proof:** (Note $\phi(p) = p - 1$)

- Being coprime to $p^a$ is the same as being coprime to $p$.
- The integers $k \leq p^a$ are precisely the integers $\leq p^a$ which are multiples of $p$.
Thus $\phi(p^a) = p^a - p^{a-1}$

**Theorem:** $\phi(m) = m \prod_{p \mid m} (1 - 1/p)$

**Proof:** $\phi(m) = p_1^{a_1}(1 - 1/p_1) \cdots p_n^{a_n}(1 - 1/p_n)$

$$= p_1^{a_1} \cdots p_n^{a_n} \prod_{p \mid m} (1 - 1/p) = m \prod_{p \mid m} (1 - 1/p)$$
Theorem: Let \( m = p_1^{a_1} \ldots p_n^{a_n} \) with \( p_i \) distinct.

\[
\begin{align*}
\Omega(m) &= \prod_{i=1}^{n} (a_i + 1) \\
\sigma(m) &= \prod_{i=1}^{n} \left( \frac{p_i^{a_i+1}}{p_i - 1} \right)
\end{align*}
\]

Proof: As before it is enough to compute \( \sigma(p^a) \) and \( \Omega(p^a) \).

The divisors of \( p^a \) are \( \{1, p, p^2, \ldots, p^a\} \).

In particular \( p^a \) has \( a+1 \) divisors thus \( \Omega(p^a) = p + 1 \).

\[
\sigma(p^a) = 1 + p + \ldots + p^a = \frac{p^{a+1} - 1}{p - 1} \quad \text{by the formula for the sum of terms in a geometric progression.}
\]

\[ \Box \]

Example: \( m = 160 = 2^5 \cdot 5^1 \)

\[
\sigma(m) = \frac{2^6 - 1}{2 - 1} \cdot \frac{5^2 - 1}{5 - 1} = 7 \cdot 31 = 217
\]

\[
\Omega(m) = (2+1)(2+1) = 9
\]

Example: \( \sum_{d|m, \, u>0} \phi(d) = m \)

\[ m = 12 \] has divisors \( 1, 2, 3, 4, 6, 12 \)

\[ \phi(1) = 1, \quad \phi(2) = 1, \quad \phi(3) = 2, \quad \phi(4) = 2, \quad \phi(6) = 2, \quad \phi(12) = 4 \]

and \[ 1 + 1 + 2 + 2 + 2 + 4 = 12 \] as expected
Thm: Let \( m > 0 \). Then \( \sum_{d|m} \phi(d) = m \).

Proof: \( F(m) = \sum_{d|m} \phi(d) \) is a multiplicative function because \( \phi(m) \) is. Thus \( F(m) = F(p_1^{a_1} \cdots p_k^{a_k}) = F(p_1^{a_1}) \cdots F(p_k^{a_k}) \).

Note that
\[
F(p^a) = \sum_{0 \leq i \leq a} \phi(p^i) = 1 + (p-1) + (p^2 - p) + \cdots + (p^a - p^{a-1}) = p^a - \phi(p^a) = p^a.
\]
Thus \( F(m) = p_1^{a_1} \cdots p_k^{a_k} = m \).

Example:

\( m = 12 \) has divisors 1, 2, 3, 4, 6, 12.

\( \phi(1) = 1, \phi(2) = 1, \phi(3) = 2, \phi(4) = 2, \phi(6) = 2, \phi(12) = 4 \)

and \( 1 + 1 + 2 + 2 + 2 + 4 = 12 \) as expected.
Perfect Numbers

*Def*: A number $m \in \mathbb{N}$ is called "perfect" if $\sigma(m) = 2m$.

*Ex*: $m = 6, \{1, 2, 3, 6\}, \sigma(6) = 1 + 2 + 3 + 6 = 12$  
$m = 28, \{1, 2, 4, 7, 14, 28\}, \sigma(28) = 1 + 2 + 4 + 7 + 14 + 28 = 56$

*Def*: We call $\Pi_m = 2^m - 1$ the $m$-th Mersenne number. If $\Pi_m$ is prime we say Mersenne prime.

*Thm*: If $\Pi_m$ is prime then $m$ is prime.

*Proof*: Suppose $m = a \cdot b$ with $1 < a, b < m$, $2^b - 1 = (2^a - 1)(2^a + 2^a + \ldots + 2^a + 1)$, with both factors $> 1$. Thus $\Pi_m$ is not prime.

*Example*:  
$2^5 - 1 = 31$ is prime  
$2^7 - 1 = 127$ is prime  
$2^{11} - 1 = 2047 = 23 \cdot 89$ not prime
There is a 1-1 correspondence between Mersenne primes and even perfect numbers.

**THM:** Let $m \in \mathbb{N}$. Then $m$ is an even perfect number if and only if $m = 2^{p-1} (2^p - 1)$ where $2^p - 1$ is a prime number.

**Proof:**

$\iff$ Let $p$ and $2^p - 1$ be primes.

Write $m = 2^{p-1} (2^p - 1)$ and compute

$\sigma(m) = \sigma(2^{p-1} (2^p - 1))$

$= \sigma(2^{p-1}) \sigma(2^p - 1) =$ \text{(by the formula)}

$= (2^{p-1}) \cdot (2^p - 1) = 2^p (2^{p-1}) (2^{p-1} - 1) = 2m$
Let \( m \) be an even perfect number.

Write \( m = 2^a \cdot b \) with \( a, b \in \mathbb{Z}_{\geq 0}, \ b \ \text{odd, } a \geq 1 \).

- \( \sigma(m) = \sigma(2^a) \cdot \sigma(b) = \left( \frac{2^{a+1} - 1}{2 - 1} \right) \cdot \sigma(b) = (2^{a+1} - 1) \cdot \sigma(b) \)

Since \( m \) is perfect \( \sigma(m) = 2m = 2(2^a \cdot b) = 2 \cdot 2^a \cdot b \)

\( \Rightarrow (2^{a+1} - 1) \cdot \sigma(b) = 2 \cdot 2^a \cdot b \quad (\star) \)

\[ 2^{a+1} \mid \sigma(b) \iff \sigma(b) = 2 \cdot 2^a \cdot c \quad (\Delta) \]

- Substituting in \( (\star) \) gives

\[ (2^{a+1} - 1) \cdot 2^{a+1} \cdot c = 2^{a+1} \cdot b \Rightarrow (2^{a+1} - 1) \cdot c = b \cdot 2^{a+1} \quad (\star\star) \]

We will now show that \( c = 1 \). Suppose \( c > 1 \).

By \( (\star\star) \) we see that \( b \) has at least three positive divisors \( 1, c, b \) thus \( \sigma(b) = 1 + b + c \),

but \( \sigma(b) = 2^{a+1} \cdot c = 2^{a+1} - 1 \cdot c + c = b + c \)

which is a contradiction thus \( c = 1 \).

Now \( (\star\star) \Rightarrow b = 2^{a+1} - 1 \) and \( (\Delta) \) gives

\[ \sigma(b) = 2^{a+1} - 1 = b + 1 \Rightarrow b \] is a prime number

thus \( m = 2^a \cdot b = 2^a (2^{a+1} - 1) \) when \( 2^{a+1} - 1 \) is prime.
**Theorem:** Let $p$ be an odd prime. Then any divisor of $M_p = 2^p - 1$ is of the form $2kp + 1$.

**Proof:** Let $q | M_p$. Since product of number of the form $2pk + 1$ is of this form we can assume $q$ is prime.

- By FLT $2^{q-1} \equiv 1 \pmod{q} \implies q | 2^{q-1} - 1 \implies q \mid (2^{p-1}, 2^{q-1} - 1)$

$$\implies q \mid (2^{p-1}, 2^{q-1} - 1) = 2^{(p, q-1)} - 1 \neq 1$$

[Claim (4): $$(a - 1, b - 1) = (a, b) - 1$$]

\[\text{See lemma 4.3 p. 166}\]

$$\implies (p, q-1) \neq 1 \implies p | q - 1 \text{ because } p \text{ is prime}$$

- Write $q - 1 = pk^l$ with $k^l = 2xK$ because $q$ is odd.

Thus $q = 2Kp + 1$

**Example:** Is $M_{23} = 2^{23} - 1 = 8388607$ a prime?

We only have to test divisibility by primes of the form $q = 46K + 1$ by the Theorem.

The smallest $q$ is 47.

Division shows that $M_{23} = 47 \cdot 174481$
**Lemma:** Let \( \mathbb{Z}_0 \) be odd. Then there is a 1-1 correspondence between factorizations of \( m \) into 2 positive odd numbers and differences of squares that equal \( m \).

**Proof:** Let \( m = a \cdot b \), where \( a, b \) are odd.

Let \( s = \frac{a+b}{2} \) and \( t = \frac{a-b}{2} \)

We check \( s^2 - t^2 = a \cdot b = m \)

Conversely, \( m = s^2 - t^2 = (s-t)(s+t) \)

gives the desired factors.

How it works:

1. Let \( m \in \mathbb{Z}_0 \) be odd.
2. (i) Find the smallest integer \( t \geq \sqrt{m} \)
3. (ii) Consider the sequence of numbers

\[ t^2 - m, (t+1)^2 - m, (t+2)^2 - m, \ldots \]

until a perfect square \( s_0^2 \) is found.
4. (iii) We have \( t_0^2 - m = s_0^2 \)

thus \( m = t_0^2 - s_0^2 = (t_0 + s_0)(t_0 - s_0) \)
Example: \( m = 6077 \)

(i) the smallest integer \( x \) such that \( x^2 > \sqrt{m} \) is 78

(ii) \( 78^2 - 6077 = 7 \)
\( 77^2 - 6077 = 164 \)
\( 80^2 - 6077 = 323 \)
\( 81^2 - 6077 = 22^2 \)

(iii) We have \( 6077 = 81^2 - 22^2 \)
\( = (81 - 22)(81 + 22) = 59 \cdot 103 \)

Remark: The procedure in (ii) will terminate because
\[ m = \left( \frac{m+1}{2} \right)^2 - \left( \frac{m-1}{2} \right)^2 = \left( \frac{m+1}{2} \right)^2 - \frac{m}{2} = \left( \frac{m-1}{2} \right)^2 \]
and \( \frac{m+1}{2} > \sqrt{m} \)

Corollary: Successive applications of Fermat's factorization will factor \( m \) completely.

In particular, if \( m = p \cdot q \) only one application suffices.
Problem 4 (Section 7.1)

Find all positive \( m \) such that \( \phi(m) \) is equal to

a) 1  

Solution: Let \( m = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} \) distinct

Recall \( \phi(m) = \prod_{i=1}^{k} p_i^{a_i-1} (p_i-1) \)

a) Suppose \( \phi(m) = 1 \).

Then \( p_i^{a_i-1} (p_i-1) = 1 \Rightarrow p_i - 1 = 1 \Rightarrow p_i = 2 \).

Thus \( a_i = 1 \) or \( m = 2^a \) \( a \geq 1 \)

\( \Rightarrow \phi(m) = 2^{a-1} = 1 \Rightarrow a = 1 \Rightarrow m = 2 \)

b) Suppose \( \phi(m) = 2 \). (Thus \( m \geq 1 \))

Then \( p_i^{a_i-1} (p_i-1) \mid 2 \Rightarrow p_i - 1 = 1 \Rightarrow 2 \)

\( \Rightarrow p_i = 2 \) or \( p_i = 3 \). \( \Rightarrow m = 2^a \cdot 3^b \)

If \( b \geq 2 \) then \( b-1 \mid 2 \) impossible.

\( \Rightarrow b = 0 \) or \( b = 1 \)

We can now divide into cases
Case 1: \( b = 1 \):

\[
m = 2^a \cdot 3 \Rightarrow \phi(m) = 2^{a-1} \cdot 2 = 2
\]

\[
a - 1 \Rightarrow 2 = 1 \Rightarrow a = 1 \Rightarrow m = 6
\]

If \( a = 0 \) \( \Rightarrow m = 3 \Rightarrow \phi(m) = 2 \cdot 1 \Rightarrow \checkmark \)

Case 2: \( b = 0 \):

\[
m = 2^a \cdot \phi(m) = 2^{a-1} = 2 \Rightarrow a = 2 \Rightarrow m = 4
\]

Thus \( \phi(m) = 2 \iff m = 3, 4, 6 \)

c) Suppose \( \phi(m) = 3 \).

Then \( p_i - 1 \mid 3 \Rightarrow p_i - 1 = 3 \text{ or } p_i = 2 = 1 \)

\[
\Rightarrow p_i = 2 \Rightarrow m = 2^a \Rightarrow \phi(m) = 2^{a-1} \neq 3
\]

There are no integers \( m \) s.t. \( \phi(m) = 3 \).