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

Q1: Let $a \in \mathbb{Z}$ be coprime to the prime $p$. What is a power of $a$ is guaranteed to be congruent to 1 mod $p$?

A: $p-1$ by FLT

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

A: Given by Euler's Theorem.

We need a preliminary definition.

**Def:** Let $m \geq 2$. The Euler $\phi$-function is given by

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

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

**Example:**
- $\phi(1) = 1$
- $\phi(2) = 1$
- $\phi(3) = 2$ because 1, 2 are coprime to 3
- $\phi(6) = 2$ because 1, 2, 3, 5 are coprime to 6
  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 \( a_1 a_2 \cdots a_{\phi(m)} \) are \( \phi(m) \)
integers s.t. \( (a_i a_j, m) = 1 \) and no two of
them are congruent modulo \( m \).

Therefore,
\[
(a_1 a_1) (a_1 a_2) \cdots (a_1 a_{\phi(m)}) \equiv a_1 a_2 \cdots a_{\phi(m)} \pmod{m}.
\]

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

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.

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

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

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

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

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

\[\Rightarrow a_i \equiv a_j \pmod{m}\] 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 \(a \in \mathbb{Z}\), \((a, m) = 1\).

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 φ):** Let \( m = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n} \).

Then \( \phi(m) = m \left( 1 - \frac{1}{p_1} \right) \left( 1 - \frac{1}{p_2} \right) \cdots \left( 1 - \frac{1}{p_n} \right) \).

**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:** \( 3 \pmod{100} \) because \( 3 = 3 \equiv 1 \pmod{100} \), \( 50 = 40 + 10 \).

3 \equiv 3 \cdot 3 \equiv 9 \cdot 3 \equiv \frac{1}{2} \cdot 9 \equiv 49 \pmod{100} \)

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

Let \( m = p_1^{a_1} \cdots p_n^{a_n} \). Then \( \phi(m) = \prod_{j=1}^{k} p_j^{a_j - 1} (p_j - 1) \).

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

\( p_j = 7 \) otherwise \( p_j - 1 = 6 \mid \phi(m) = 8 \) impossible. Thus \( m = 2 \cdot 3 \cdot 5 \).

Moreover \( b = 0 \) or \( b = 1 \) otherwise \( 3 \mid 8 \); similarly \( c = 0 \) or \( c = 1 \).

Now we have 4 cases to check:

1. \( b = c = 0 \Rightarrow m = 2^a \Rightarrow \phi(m) = 2^{a-1} = 8 \Rightarrow a = 4 \Rightarrow m = 16 \)
2. \( b = 0, c = 1 \Rightarrow m = 2^a \cdot 5 \Rightarrow \phi(m) = 2^{a-1} \cdot 4 = 8 \Rightarrow a = 2 \Rightarrow m = 20 \)
3. \( b = 1, c = 0 \Rightarrow m = 2^a \cdot 3 \Rightarrow \phi(m) = 2^{a-1} \cdot 2 = 8 \Rightarrow a = 3 \Rightarrow m = 24 \)
4. \( b = c = 1 \Rightarrow m = 2^a \cdot 3 \cdot 5 \Rightarrow \phi(m) = 2^{a-1} \cdot 2 \cdot 4 = 8 \Rightarrow a = 1 \Rightarrow m = 30 \)

If \( a = 0 \) then \( m = 15 \) and \( \phi(m) = 8 \) also works!
LECTURE 16

**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. \( \phi(m) \) "the Euler \( \phi \)-function"
4. \( \tau(m) = \text{"number of positive divisors of } m \text{"} \)
5. \( \sigma(m) = \text{"sum of positive divisors of } m \text{"} \)

**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 \( f(m_1 \cdot m_2) = f(m_1) \cdot f(m_2) \quad \forall m_1, m_2 \)
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:

<table>
<thead>
<tr>
<th>1</th>
<th>( m_1 + 1 )</th>
<th>2 ( m_1 + 1 )</th>
<th>\ldots</th>
<th>(( m_2 - 1 )) ( m_1 + 1 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>( m_1 + 2 )</td>
<td>2 ( m_1 + 2 )</td>
<td>\ldots</td>
<td>(( m_2 - 1 )) ( m_1 + 2 )</td>
</tr>
<tr>
<td>3</td>
<td>( m_1 + 3 )</td>
<td>2 ( m_1 + 3 )</td>
<td>\ldots</td>
<td>(( m_2 - 1 )) ( m_1 + 3 )</td>
</tr>
<tr>
<td>\vdots</td>
<td>\vdots</td>
<td>\vdots</td>
<td>\ldots</td>
<td>\vdots</td>
</tr>
<tr>
<td>( n )</td>
<td>( m_1 + n )</td>
<td>2 ( m_1 + n )</td>
<td>\ldots</td>
<td>(( m_2 - 1 )) ( m_1 + n )</td>
</tr>
<tr>
<td>( m_1 )</td>
<td>2 ( m_1 )</td>
<td>3 ( m_1 )</td>
<td>\ldots</td>
<td>( m_1 \cdot m_2 )</td>
</tr>
</tbody>
</table>

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 $m_1 \cdot m_2$.

This is a method to produce multiplicative functions.

**Theorem:** Let $f$ be an arithmetic function. Define the arithmetic 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 multiplicative.
**Theorem:** $\sigma(m)$ 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. \[\Box\]
ARITHMETIC FUNCTIONS CONTINUED

**Theorem.** Let \( f \) be an arithmetic function. Define the function \( F \) by

\[
F(m) = \sum_{d \mid m, d > 0} f(d) \quad \forall m \in \mathbb{Z}_{+}
\]

If \( f \) is multiplicative, then \( F \) is also multiplicative.

**Corollary.** \( \tau(m) \) and \( \sigma(m) \) are multiplicative functions.

**Proof of Theorem:**

\[
\text{WANT: } F(m_1 \cdot m_2) = F(m_1) \cdot F(m_2)
\]

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

We have

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

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

Thus

\[
F(m_1 \cdot m_2) = \sum_{d | (m_1, m_2)} f(d) = \sum_{d | (d_1, d_2)} f(d_1, d_2)
\]

\[
= \sum_{d_1 | m_1, d_2 | m_2} f(d_1) \cdot f(d_2) = \left(\sum_{d_1 > 0} f(d_1)\right) \left(\sum_{d_2 > 0} f(d_2)\right) = F(m_1) \cdot F(m_2) \]
Formulas for $\phi_1, \phi_2, \phi_3$

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

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

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

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

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

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

Being coprime to $p^a$ is the same as being coprime to $p$.

The integers $kp$ with $1 \leq k \leq p^{a-1}$ are precisely the integers $\leq p^a$ which are multiples of $p$. Thus $\phi(p^a) = p^a - p$

Then: $\phi(m) = m \prod_{p|m} \left(1 - \frac{1}{p} \right)$

**Proof:**

$$\phi(m) = p_1^{a_1} (1 - \frac{1}{p_1}) \cdots p_k^{a_k} (1 - \frac{1}{p_k})$$

$$= p_1^{a_1} \cdots p_k^{a_k} \left(1 - \frac{1}{p_1} \right) \cdots \left(1 - \frac{1}{p_k} \right) = m \prod_{p|m} \left(1 - \frac{1}{p} \right)$$
**Theorem:** Let \( m = p_1^{a_1} \cdot \ldots \cdot p_n^{a_n} \) with \( p_i \) distinct.

\[
\begin{cases}
\mathcal{Z}(m) = \prod_{i=1}^{n} (a_i + 1) \\
\sigma(m) = \prod_{i=1}^{n} \left( \frac{p_i^{a_i+1} - 1}{p_i - 1} \right)
\end{cases}
\]

**Proof:** As before it is enough to compute \( \sigma(p^a) \) and \( \mathcal{Z}(p^a) \).

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

In particular \( p^a \) has \( a+1 \) divisors thus \( \mathcal{Z}(p^a) = a+1 \).

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

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

\[\sigma(m) = \frac{2^6 - 1}{2^5 - 1} \cdot \frac{5^3 - 1}{5^2 - 1} = 7 \cdot 31 = 217 \]

\[\mathcal{Z}(m) = (2+1)(2+1) = 9 \]

**Example:** \( \sum_{d\mid m} \phi(d) = m \)

- \( m = 12 \) 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.
**Thm:** Let \( m > 0 \). Then \( \sum_{\substack{d | m \atop d > 0}} \phi(d) = m \)

**Proof:** \( F(m) = \sum_{\substack{d | m \atop d > 0}} \phi(d) \) 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

\[
F(p^a) = \sum_{0 \leq i \leq a} \phi(p^i) = 1 + (p-1) + (p^2-p) + \ldots + (p^a-p^{a-1}) = p^a
\]

Thus \( F(m) = p_1^{a_1} \cdots p_k^{a_k} = m \)

\( \square \)

**Example:**

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

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

\( \phi(12) = 4 \)

and \( 1 + 1 + 2 + 2 + 2 + 4 = 12 \) as expected!